TRADOC DCSINT Handbook No. 1

A Military Guide to

Terrorism

in the Twenty-First Century

US Army Training and Doctrine Command
Deputy Chief of Staff for Intelligence
Assistant Deputy Chief of Staff for Intelligence - Threats
Fort Leavenworth, Kansas

2004

Version 2.0

Report Documentation Page

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **00 AUG 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**	
4. TITLE AND SUBTITLE **A Military Guide to Terrorism in the Twenty-First Century, TRADOC DCSINT Handbook No.1, Version 2.0**		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)		5d. PROJECT NUMBER	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army Training and Doctrine Command, Dep Chief of Staff for Intelligence, Asst Deputy Chief of Staff for Intelligence - Threats, Fort Leavenworth, KS**		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**			
13. SUPPLEMENTARY NOTES **The original document contains color images.**			
14. ABSTRACT			
15. SUBJECT TERMS			

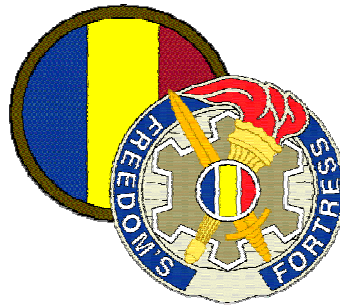| 16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **UU**	18. NUMBER OF PAGES **364**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Page Intentionally Blank

A Military Guide to

Terrorism

in the Twenty-First Century

U.S. Army Training and Doctrine Command
Deputy Chief of Staff for Intelligence
Assistant Deputy Chief of Staff for Intelligence – Threats

12 October 2004
Version 2.0

ACKNOWLEDGEMENTS
Threats Terrorism Team (T3) Network

A Military Guide to Terrorism in the 21st Century

Table of Contents

Page Intentionally Blank

Preface

A Military Guide to Terrorism in the Twenty-First Century is a reference guide prepared under the direction of the U.S. Army Training and Doctrine Command, Assistant Deputy Chief of Staff for Intelligence-Threats. Understanding terrorism spans foreign and domestic threats of nation-states, rogue states with international or transnational agent demonstrations, and actors with specific strategies, tactics, and targets. A central aspect of this terrorism guide comprises foreign and domestic threats against the United States of America in a contemporary operational environment (COE).

Purpose. This informational handbook supports operational missions, institutional training, and professional military education for U.S. military forces in the Global War on Terrorism (GWOT). This capstone document provides an introduction to the nature of terrorism and recognition of terrorist threats to U.S. military forces. A common situational awareness by U.S. military forces considers three principal venues: forces that are deployed, forces that are in transit to or from an operational mission, and forces that are primarily installation or institution support.

Intended Audience. This handbook exists primarily for U.S. military forces, however, other applicable groups include interagency, intergovernmental, civilian contractor, non-governmental, private volunteer, and humanitarian relief organizations. Compiled from open source materials, this handbook promotes a "Threats" perspective and enemy situational awareness of U.S. strategies and operations in combating terrorism. Neither a counter-terrorism directive nor anti-terrorism manual, the handbook complements but does not replace training and intelligence products on terrorism.

Handbook Use. Study of contemporary terrorist behavior and motivation, terrorist goals and objectives, and a composite of probable terrorist tactics, techniques, and procedures (TTP) improves readiness of U.S. military forces. As a living document, this handbook will be updated as necessary to ensure a current and relevant resource. A selected bibliography presents citations for detailed study of specific terrorism topics. Unless stated otherwise, masculine nouns or pronouns do not refer exclusively to men.

Proponent Statement. Headquarters, U.S. Army Training and Doctrine Command (TRADOC) is the proponent for this publication. Periodic updates will accommodate emergent user requirements on terrorism. Send comments and recommendations on DA Form 2028 directly to TRADOC Assistant Deputy Chief of Staff for Intelligence – Threats at the following address: Director, TRADOC ADCSINT – Threats, ATTN: ATIN-L-T (Bldg 53), 700 Scott Avenue, Fort Leavenworth, Kansas 66027-1323. This handbook is available at Army Knowledge Online (**www.us.army.mil**). Additionally, the General Dennis J. Reimer Training and Doctrine Digital Library (www.adtdl.army.mil) lists the handbook as a special text.

Page Intentionally Blank

Introduction

A Military Guide to Terrorism in the Twenty-First Century is a capstone reference guide that describes terrorism[1] and its potential impact on U.S. military forces in the conduct of mission operations. The handbook highlights the nature of terrorism present in a full spectrum contemporary operational environment (COE),[2] and the likely impacts on the conduct of U.S. military operations.

Terrorism has become one of the most pervasive and critical threats to the security of the United States in recent history. U.S. military fatalities from terrorist actions between 1980 and 2002 exceed the total battle deaths from Operations Urgent Fury (Grenada), Just Cause (Panama), and Desert Shield/ Storm (Persian Gulf).[3] As Chart Intro-1 depicts, there were 672 military deaths between 1980 and 2002 attributed to either hostile action or terrorism. Of these deaths, 63% were due to terrorist actions.[4]

Since these Department of Defense figures only go through 2002, they do not include all the casualties from Operation Enduring Freedom (OEF), or any of the casualties from Operation Iraqi Freedom (OIF). As of 25 September 2004, OEF reported 56 hostile deaths since 7 October 2001.[5] Figures for OIF as of 25 September 2004 indicate a total of 791 hostile deaths, 109 occurring during major combat operations that terminated on 30 April 2003, and 682 occurring after the end of major combat operations.[6]

Although many of these deaths are attributed to combat operations, many were caused by terrorist actions in these two theaters. On occasion, adversary combatant forces have adopted terrorist tactics to continue their fight when they no longer possess the ability to conduct conventional engagement attacks. Time will only tell how DOD will officially categorize the casualties. In the 2003 State Department *Patterns of Global Terrorism* Report, the State Department did make a distinction between military operations and terrorist attacks. Those attacks directed at combatants are not classified as terrorist attacks, whereas those against noncombatants (civilians and military personnel who at the time of the incident were unarmed and/or not on duty) were classified as terrorist attacks. The fact remains, though, that terrorism has been a major threat to the security of our armed forces for a number of years.

---

[1] Joint Publication 1-02. *Department of Defense Dictionary of Military Terms and Associated Terms*, 12 April 2001, as amended through 9 June 2004.

[2] U.S. Army Field Manual FM 7-100, Opposing Force Doctrinal Framework and Strategy, May 2003, iv to xvi.

[3] Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, *Table 13, Worldwide U.S. Active Duty Military Deaths, Selected Military Operations* (Washington, D.C., n.d.); available from http://web1.whs.osd.mil/mmid/casualty/table13.htm; Internet; accessed 6 July 2004.

[4] Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, U.S. Active Duty Military Deaths – 1980 through 2002 (Washington, D.C., As of 10 April 2003); available from http://web1.whs.osd.mil/mmid/casualty/Death_Rates.pdf; Internet; accessed 6 July 2004.

[5] Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, *Global War on Terrorism – Casualty Summary Operation Enduring Freedom* (Washington, D.C., As of 25 September 2004); available from http://web1.whs.osd.mil/mmid/casualty/WOTSUM.pdf; Internet; accessed 4 October 2004.

[6] Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, *War on Terrorism – Operation Iraqi Freedom, By Casualty Category Within Type* (Washington, D.C., As of 25 September 2004); available from http://web1.whs.osd.mil/mmid/casualty/OIF-Total.pdf; Internet; accessed 4 October 2004.

However, despite its consistent menace, terrorism is a threat that is poorly understood, and frequently confusing due to widely divergent views over exactly what defines terrorism.

Chart Intro-1: U.S. Active Duty Military Deaths 1980-2002

Total Deaths due to Terrorism = 426

Total Deaths due to Hostile Action = 246

Legend: Hostile Deaths, Terrorist Deaths

Y-axis: Deaths (0 to 450)

X-axis: Year (1980 to 2002, Total)

Data values shown: 426, 263, 246, 147, 55, 37, 29, 23, 19, 18, 17, 17, 6, 5, 3, 2, 1, 0, 7

(*Source:* Department of Defense)
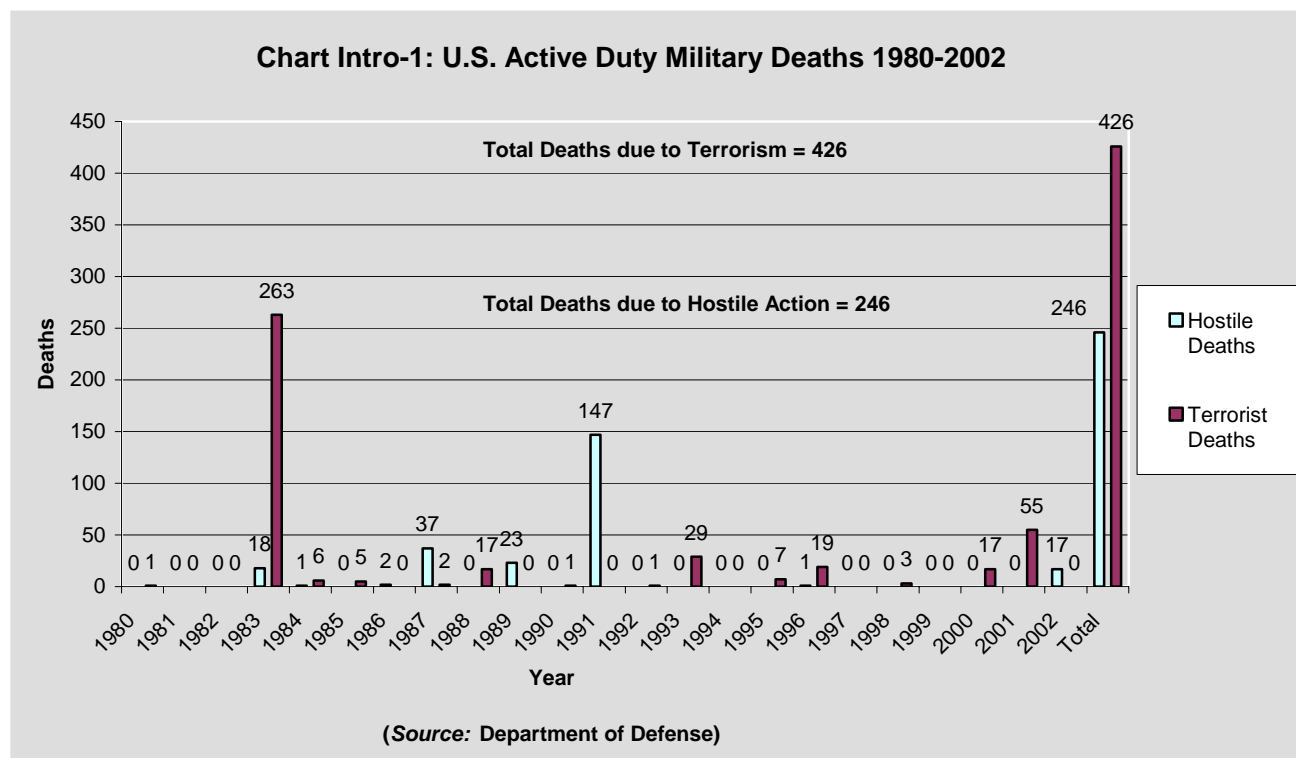
Terrorism, as discussed in this handbook, centers on the known principal terrorist "Threats" to the United States of America. The United States confronts terrorism in daily circumstances, both foreign and domestic; and prepares for security against terrorism expected in the foreseeable future. Of these threats, the most significant U.S. concerns are terrorist organizations with demonstrated global reach capabilities and those terrorist organizations that seek to acquire and use weapons of mass destruction (WMD). Nonetheless, the threat of terrorism to the U.S. is present across the entire spectrum of conflict. The use of terrorism ranges from individual acts of wanton damage or destruction to property or person, to highly sophisticated operations conducted by highly organized violent groups with social, environmental, religious, economic, or political agendas. This full range of terrorist activity can have significant negative impact on the conduct of missions by U.S. military forces.

Scope of the Issue

Terrorism is a significant challenge for U.S. military forces in the twenty-first century. Terrorist violence has changed in recent years from an agenda-forcing and attention-getting tool of the politically disenfranchised to a significant asymmetric form of conflict employed

against adversaries of greater economic, military, and political strength. While terrorist acts may have been seen as extraordinary several decades ago, today terrorism demonstrates a profound impact on populations at the local, regional, national, and international levels.

Terrorism is defined by DOD as: "The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."[7] This is not a universally accepted definition outside of the Department of Defense, and the study of terrorism has often been mired in a conflict over definitions and semantics. This is examined in Chapter 1, but for the purposes of this DOD document, this doctrinal definition will be used unless otherwise noted.

Terrorism is a special type of violence; while it has a political element, it is a criminal offense under nearly every national or international legal code. Although terrorism has not yet caused the physical devastation and large number of casualties normally associated with traditional warfare, it often produces a significant adverse psychological impact and presents a greater threat than a simple reckoning of the numbers killed or the quantity of materiel destroyed would indicate.[8] An excellent example of this is the impact on the United States of the 9/11 attacks and the following anthrax incidents. For many people around the U.S., these attacks weakened their sense of safety and security. This first experience of catastrophic terrorism was evidence that the United States was not immune to attacks by international or transnational terrorist groups. Ultimately, these attacks also had severe economic impacts on the country. As Brian Jenkins testified to the 9/11 Commission, "The September 11 attack produced cascading economic effects that directly and indirectly have cost the United States hundreds of billions of dollars."[9] For other citizens, though, these terrorist acts fortified their will and resolve. Consequently, a national resolve emerged from these catastrophic incidents to combat terrorism and reassert confidence in the economy.

Successful in attracting attention and creating fear and anxiety, terrorist acts often fail to translate into concrete long-term gains or achieve an ultimate objective.[10] Escalating acts of terrorism can be self-defeating when the acts become so extreme that public reaction loses attention on the terrorist's intended purpose and focuses on the acts rather than the political issue. The example of Palestinian defiance to Israeli controls in this geographic region of the Mideast illustrates how progressively more violent acts of resistance or terrorism can sometimes alienate large sections of public opinion that once may have supported a Palestinian search for recognition.[11] Thus, as a tactic, terror can be successful in immediate purpose, but fail in achieving its ultimate aim unless dedicated political or military efforts

---

[7] FM 100-20, *Military Operations in Low Intensity Conflict*, 5 December 1990; and Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 9 June 2004.

[8] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 33-34.

[9] National Commission on Terrorist Attacks Upon the United States, Statement of Brian Jenkins to the Commission, March 31, 2003; available from http://www.9-11commission.gov/hearings/hearing1/witness_jenkins.htm; Internet; accessed 23 September 2004.

[10] Caleb Carr, *The Lessons of Terror: A History of Warfare Against Civilians: Why it has Always Failed and Why it will Fail Again* (New York: Random House, 2002), 11.

[11] Caleb Carr, "TIME.com Interview with Calib Carr," 1 February 2002; available at http://www.time.com/time/2002/carr/interview.html; Internet; accessed 31 August 2004.

coincide to produce tangible results. [12]   When the threat or use of terrorism is used in coordination with elements such as political or military power, strategic impact may be successful. Some may see the struggle for Algerian independence or Israeli independence as strategic outcomes that used terrorism as a major instrument of influence. Others may see the 2004 Spanish withdrawal from coalition forces in Iraq as an operational outcome of terrorism in Spain, and a means toward strategic terrorist aims of fracturing the coalition and eventually causing removal of U.S. presence and prestige in the Mideast.

"Many potential adversaries, as reflected in doctrinal writings and statements, see U.S. military concepts, together with technology, as giving the United States the ability to expand its lead in conventional warfighting capabilities.

This perception among present and potential adversaries will continue to generate the pursuit of asymmetric capabilities against U.S. forces and interests abroad as well as the territory of the United States. U.S. opponents—state and such nonstate actors as drug lords, terrorists, and foreign insurgents—will not want to engage the U.S. military on its terms. They will choose instead political and military strategies designed to dissuade the United States from using force, or, if the United States does use force, to exhaust American will, circumvent or minimize U.S. strengths, and exploit perceived U.S. weaknesses. Asymmetric challenges can arise across the spectrum of conflict that will confront U.S. forces in a theater of operations *or on U.S. soil*."

National Intelligence Council's "Global Trends 2015: A Dialogue About the Future With Nongovernment Experts" Report, December 2000.

Purpose

This handbook serves as an unclassified resource to inform U.S. military members of the nature and characteristics of terrorism. The intention is to create a situational awareness and understanding of current terrorism capabilities and limitations, and complement the deliberate processes of military risk management, force protection, and mission orders conduct and leader decision-making. From a "Threats" perspective, terrorism *capabilities and limitations* indicate possible and probable types of threat action that may be directed against U.S. military members and units. Commanders, organizational leaders, and all other military unit members can use this handbook to:

---

[12] Walter Lacquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (New York: Oxford University Press, 1999), 48.

- Understand the nature of the terrorist threat through a concise historical review of terrorism, and basic descriptions of methods and organizational structures commonly used by terrorist organizations.

- Understand terrorist goals, objectives, and conduct of terrorist operations. Acknowledging that asymmetric operations provide a significant advantage to the terrorist, study of situational patterns and techniques in terrorism over time can offer insight and possible trends for future attacks.

- Understand the threat of terrorism to U.S. military forces, equipment, and infrastructure.

- Identify appropriate levels of force protection (FP), operational security (OPSEC), and terrorism countermeasures based upon unit status and situation.

- Provide relevant terrorism information that applies to Active Component (AC) and Reserve Component (RC) Federal Reserves and state National Guard forces in primary scenarios of being deployed on a mission, being deployable or in transit for an operational mission, or being a nondeployable military force that is designated as installation or institutional support.

This handbook is not intended to be a counterterrorism "how-to" manual, or to replace current training and intelligence products. Its intent is to provide a base of knowledge that will allow better understanding and employment of existing resources.

U.S. Strategic Overview

Defending the Nation against its enemies is the first and fundamental commitment of the Federal Government. The National Military Strategy (2004) describes ways and means for Joint Forces to protect the U.S. and win the "War on Terrorism." U.S. Joint Forces assist the Nation in preventing conflict or surprise attack, while concurrently transforming military capabilities while at war and preparing to meet future global challenges. In this contemporary operational environment, two primary U.S. concerns are terrorists of global reach and the emergent threat of terrorist use of weapons of mass destruction. The National Security Strategy (NSS) of the USA states national priorities for dealing with terrorism.

When the President of the United States of America addresses terrorism as an enemy, the enemy is not a single political regime or person or religion or ideology. "The enemy is terrorism – premeditated, politically motivated violence perpetrated against innocents…[U.S.] priority will be first to disrupt and destroy terrorist organizations of global reach and attack their leadership; command, control, and communications; material support; and finances."[13] The strategic intent of the U.S. National Strategy for Combating Terrorism adds a national priority of denying sanctuary to terrorist organizations with global reach.[14]

---

[13] President, National Strategy, "National Security Strategy of the United States of America," Washington, D.C. (December 2002): Introduction and Section III; available from http://www.whitehouse.gov/nsc/print/nssall.html; Internet; accessed 8 December 2003.
[14] President, National Strategy, "National Strategy for Combating Terrorism," Washington, D.C. (February 2003): 11; available from http://www.state.gov/s/ct/rls/rm/2003/17798.htm; Internet; accessed 8 December 2003.

Other principal threats are rogue states or terrorist organizations – enemies – who have declared the intention to obtain and use weapons of mass destruction [WMD] against the United States of America. The September 2001 attacks on the United States demonstrated that inflicting mass casualties is one of several specific means that will be used by terrorists to spotlight an agenda. Mass casualties would be exponentially more severe if terrorists acquired and used weapons of mass destruction.[15] As noted in the national security strategy, the targets of these WMD attacks include U.S. military forces and civilian population.

The major institutions of American national security were designed in a different era to meet different requirements. All of these security measures are transforming. This includes building and maintaining national defenses beyond challenge…an essential role exists for American military strength in near-term readiness and the ability to fight the war on terrorism.[16]

U.S. Goals and Objectives

The United States demonstrates a national resolve to ensure the protection of the Nation and reduce its vulnerability to terrorism. Although an enduring vulnerability exists, the leaders at each level of government are implementing interconnected strategies to address emerging risks and threats of terrorism. While protection infers prevention from terrorist attacks, U.S. national strategies recognize that accepting some level of terrorism risk is a permanent condition. The National Strategy for Homeland Security presents six critical mission areas for security risk management and resourcing: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response.[17] A survey of these mission sets aligns easily with functions of expert support that U.S. military forces can provide, as an operating element of the Department of Defense, within Federal law.

Of note, the United States has implemented an integrated series of national strategies to enhance the security of the Nation. These strategies translate instruments of national power into operational and tactical action against terrorism. U.S. military forces are part of a national arsenal of capabilities among diplomatic, economic, law enforcement, financial, information, and intelligence institutions in the Global War on Terrorism (GWOT).

> **"No group or nation should mistake America's intention:**
> **We will not rest until terrorist groups of global reach have**
> **been found, have been stopped, and have been defeated."**

> George W. Bush
> President of the United States of America
> September 14, 2001

---

[15] President, National Strategy, "National Security Strategy of the United States of America," Washington, D.C. (December 2002): Section V; available from http://www.whitehouse.gov/nsc/print/nssall.html; Internet; accessed 8 December 2003.

[16] Ibid., Section IX.

[17] President, National Strategy, "National Strategy for Homeland Security," Washington, D.C. (16 July 2002): viii and 2; available from http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf; Internet; accessed 8 December 2003.

Soon after the catastrophe of the 2001 World Trade Center bombing, the President of the United States declared a specific charter to U.S. military forces: "The battle is now joined on many fronts. We will not waver, we will not tire, we will not falter and we will not fail. Peace and freedom will prevail…To all the men and women in our military, every sailor, every soldier, every airman, every coast guardsman, every marine, I say this: Your mission is defined. The objectives are clear. Your goal is just. You have my full confidence, and you will have every tool you need to carry out your duty."[18]   U.S. military forces are one of several instruments of national power. Objectives are clearly stated in mission orders. The "just" goal reaches beyond a task of preserving U.S. freedoms. This goal envisions a world with the ability for all people to live and prosper without fear.

Approach to Understanding Terrorism

The 2004 version of *A Military Guide to Terrorism in the Twenty-First Century* builds on a 2004 database of open source information with current subject updates, as well as selected expansion of special topics. Comments and recommendations from handbook users were instrumental in shaping revisions and identifying new requirements.

The preface keynotes this open source unclassified reference document on terrorism. The purpose and intended audience, although existing initially for U.S. military forces, provides a useful awareness to other activities in interagency, intergovernmental, nongovernmental, private volunteer, humanitarian relief, and civilian organizations. The introduction centers attention on reviewing historical perspectives of terrorism, understanding current vulnerabilities and terrorism threats, and considering emergent and future terrorism.

Chapter 1: ***Nature and History of Terror****,* defines the concept of terrorism and provides basic terms of reference for a common vocabulary. Attention on modern terrorism complements the historical perspective of terrorism discussed later in the handbook.

Chapter 2: ***Terrorist Behaviors, Motivations, and Characteristics****,* presents recent examples of terrorist behavior and illustrates individual or group declared ideology or philosophy. Additions expand generic profile descriptions with case examples to highlight the many types of lifestyle that can develop a terrorist's mindset and conduct.

Chapter 3: ***Terrorist Group Organization***, provides examples and diagrams of hierarchical and networked terrorist group organizations, provides an appreciation of the diverse range of terrorist capability, but also portrays organizational limitations. Discussion of U.S. domestic terrorist acts accent this homeland threat, and the ability for inter-terrorist group transfer of information and support.

Chapter 4: ***Assessing Terrorist Capabilities and Intentions****,* emphasizes risk assessment and management of U.S. military forces against terrorism. Vulnerabilities use a "red teaming" approach of potential terrorist intelligence preparation of the battlefield (IPB) against U.S.

---

[18] "Transcript of President George Bush's address 10/07/01," ATTACK on AMERICA [database on-line]; available from http://multimedia.belointeractive.com/attack/bush/1007bushtranscript.html; Internet; accessed 13 July 2004.

military forces. Appreciating terrorist intentions progresses to elements of potential terrorist reconnaissance and surveillance.

Chapter 5: **Terrorist Targeting of U.S. Military Forces,** assesses potential targeting of U.S. military forces by terrorist organizations with a situational framework of deployed, deployable and in transit, or non-deployable U.S. military forces. Discussion includes the increased overseas presence by U.S. military forces in operational missions, forward stationed forces, and cycle of transiting forces with deployments and redeployments.

Chapter 6: **Future of Terrorism,** examines the future of terrorism and the merging of terrorists with other state and sub-state entities. It also discusses some of the possible causes of future conflicts and how terrorism will be integrated into this evolution of conflict.

Appendices provide supplemental information to understanding terrorism.

A: **Terrorist Threat to Combatant Commands.** The annual publication of *Patterns of Global Terrorism 2003* by the U.S. Department of State remains the primary source for displaying terrorism threats to the five U.S. Combatant Command areas, and specific data to indicate regional and global patterns related to terrorism.

B: **Terrorist Planning Cycle.** Emphasis outlines the norms of terrorist planning and phased conduct of operations. Operations may be sequential, parallel, or simultaneous.

C: **Terrorist Operations and Tactics.** Examples describe emerging patterns in operations and inferences of preferred terrorism tactics and techniques. Descriptions expand the operating environment awareness to include land, air, and maritime terrorism scenarios.

D: **Firearms.** Illustrations, photographs, and descriptions present a survey of conventional small arms often used by terrorists. Intelligence summaries provide the basis for this sampling of hand or shoulder fired weapons.

E: **Improvised Explosive Devices.** Illustrations, photographs, and descriptions present a survey of explosive charges and trigger devices for improvised explosive devices (IED).

F: **Conventional Military Munitions.** Illustrations, photographs, and descriptions present a survey of selected conventional military munitions used by terrorists including fragmentation grenades, rocket propelled grenades, shoulder-fired SAMS, and artillery munitions.

G: **Weapons of Mass Destruction.** Discussion emphasizes multiple definitions of WMD and the underpinning of a common definition that focuses on weapon effects. Primary types of attack are chemical, biological, nuclear, radiological, and high yield explosives (CBRNE) in effects.

H: **WMD and CBRNE Consequence Management.** This appendix notes the probability of terrorist attack with CBRNE (chemical, biological, nuclear, radiological, and high yield explosive) devices and the military's support to civil authorities in these situations. The U.S. continues to expand a capability for national response to CBRNE incidents and the specter of

WMD attack. A significant capability in this WMD consequence management arsenal is U.S. Northern Command's Joint Task Force – Civil Support (JTF-CS).

I: *Cyber Operations.* Overview of the global information grid accents the indispensable nature of information technology, the use of IT by terrorists to support their operations, and the fact that our systems are high value targets of cyber terrorists and present a significant threat to both U.S. military forces and national security.

J: *Case Studies of Terrorism.* This appendix summarizes terrorist actions against the U.S. in domestic and foreign locales and highlights risk assessment and force protection requirements in the contemporary operating environment. A series of case studies promotes appreciation of the primary underlying aim of terrorism – a demoralizing psychological effect on the target population and leaders to erode resolve and to enhance terrorist objectives. Initial case study incidents include the Murrah Federal Building in Oklahoma City (1995), Khobar Towers in Saudi Arabia (1996), and the USS *Cole* in Yemen (2000).

Conclusion

This handbook provides a straightforward description of an increasingly common and heinous method of conflict – Terrorism. Promoting knowledge and awareness of terrorism enhances the ability of U.S. military forces to assess conditional vulnerabilities, determine enemy threats, dissuade and deter terrorist acts, deny use of particular terrorism means, and effectively defend against terrorist attack.[19] The U.S. National Strategy for Combating Terrorism states the campaigning along four simultaneous fronts: (1) defeat terrorist organizations of global reach through relentless action; (2) deny support to terrorism; (3) diminish the conditions that encourages terrorism; and (4) defend the people and interests of the United States of America against terrorism.[20] Knowing vulnerabilities and threats are essential to effective U.S. action.

Ultimately, terrorism can cause more than physical carnage by imprinting the psychological horror in the minds of the target audience. The aim of the terrorist, whether terrorism is viewed as a strategy or a tactic, is an attack on resolve. Therefore, the fundamental aim of terrorism is its psychological effect on man and the decisions that result.

The overarching aim of this handbook is to reinforce the will and resolve of U.S. military forces at war – a Global War on Terrorism. In a long-term war of uncertain duration, the United States of America will continue to defend its values, liberties, and culture; its economic prosperity; and its security.

---

[19] Moilanen, Jon H. "Engagement and Disarmament: A U.S. National Security Strategy for Biological Weapons of Mass Destruction," *Essays on Strategy XIII.* Mary A. Sommervile ed., Washington, D.C., National Defense University Press, 1996.

[20] President, National Strategy, "National Strategy for Combating Terrorism," Washington, D.C. (February 2003): 11, 29-30; available from http://www.state.gov/s/ct/rls/rm/2003/17798.htm; Internet; accessed 8 December 2003.

Page Intentionally Blank

Chapter 1
Nature and History of Terror

On the extremely terse end of the spectrum, the terrorism expert Brian Jenkins bluntly stated in 1974 "Terrorism is theatre." [21] This is possibly the best three-word analogy for such a complex phenomenon. Think of terrorism, like a play, as a constructed incident presented to a large audience to gain and hold their attention. Modern media provide the stage, and audience attention is further engaged because random individuals are selected to join the principals on stage as victims. And like a play, the point of the exercise is the feelings and attitudes of the audience, not the actors.

Terrorist acts or the threat of such action have been in existence for millennia. Despite having a history longer than the modern nation-state, the use of terror by governments and those that contest their power remains poorly understood. While the meaning of the word _terror_ itself is clear, when it is applied to acts and actors in the real world it becomes confusing. Part of this is due to the use of terror tactics by actors at all levels in the social and political environment. Is the Unabomber, with his solo campaign of terror, a criminal, terrorist, or revolutionary? Can he be compared to the French revolutionary governments who coined the word terrorism by instituting systematic state terror against the population of France in the 1790s, killing thousands? Are either the same as revolutionary terrorist groups such as the Baader-Meinhof Gang of West Germany or the Weather Underground in the United States?

So we see that distinctions of size and political legitimacy of the actors using terror raise questions as to what is and is not terrorism. The concept of _moral equivalency_ is frequently used as an argument to broaden and blur the definition of terrorism as well. This concept argues that the outcome of an action is what matters, not the intent.[22] Collateral or unintended damage to civilians from an attack by uniformed military forces on a legitimate military target is the same as a terrorist bomb directed deliberately at the civilian target with the intent of creating that damage. Simply put, a car bomb on a city street and a jet fighter dropping a bomb on a tank are both acts of violence that produce death and horror. Therefore (at the extreme end of this argument) any military action is simply terrorism by a different name.[23] This is the reasoning behind the famous phrase "One man's terrorist is another man's freedom fighter." It is also a legacy of legitimizing the use of terror by successful revolutionary movements after the fact.

> **"Terrorism has a purpose that goes well beyond the act itself; the goal is to generate fear."**
> **Opposing Force: Doctrinal Framework and Strategy FM 7-100 (2003)**

Finally, the significant growth in the number of causes and social contexts using terrorism combined with the flexibility and adaptability of terror throughout the years has contributed to the confusion. Those seeking to disrupt, reorder or destroy the status quo have continuously sought new and creative ways to achieve their goals. Although many of the

---

[21] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 38.
[22] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 33.
[23] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "The Terrorists' View."

tactics and techniques used by terrorism have remained somewhat the same, significant improvements in technology have resulted in more lethal means.

Despite these problems, terrorism can be studied and useful conclusions drawn. The first section of this chapter introduces a background of definitions and concepts for understanding terrorism. The second section provides a brief survey of the historical employment of terrorism. By establishing specific definitions and concrete concepts regarding terrorism, and determining how it has been used in the past, we can improve our ability to understand how it works in the present, and what it may become in the future.

Section I: What is Terrorism

Terrorism has been described variously as both a tactic and strategy; a crime and a holy duty; a justified reaction to oppression and an inexcusable abomination. Obviously, a lot depends on whose point of view is being represented. Terrorism has often been an effective tactic for the weaker side in a conflict. As an asymmetric form of conflict, it confers coercive power with many of the advantages of military force at a fraction of the cost. Due to the secretive nature and small size of terrorist organizations, they often offer opponents no clear organization to defend against or to deter. Terrorism is a means to an "end" or objective. Methods may vary from incident to incident but in review of terrorism during the last two centuries, methods appear strikingly similar in concept.

What may be of most concern is the lethality and damage that adaptive terrorists can inflict when armed with expanding technologies and intellect. That is why preemption is more important than ever before. However, deterrence and preemption can be difficult against transnational terrorist groups. As stated in an al Qaeda article in January 2002, "[Deterrence] is completely eliminated when dealing with people who do not care about living but thirst for martyrdom. While the principle of deterrence works well [in warfare] between countries, it does not work at all for an organization with no permanent bases and with no capital in Western banks…How can such people, who strive for death more than anything else, be deterred?"[24]

In some cases, terrorism has been a means to carry on a conflict without the adversary realizing the nature of the threat, mistaking terrorism for criminal activity. Because of these characteristics, terrorism has become increasingly common among those pursuing extreme goals throughout the world. But despite its popularity, terrorism can be a nebulous concept. Even within the U.S. Government, agencies responsible for different functions in our current fight against terrorism use different definitions.

> ### *Related Definitions*
> **Terrorist**: (JP 1-02)
> An individual who uses violence, terror, and intimidation to achieve a result.
> **Counter-terrorism**: (JP 1-02)
> Offensive measures taken to prevent, deter, and respond to terrorism.
> **Anti-terrorism**: (JP 1-02)
> Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

---

[24] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 12, quoting Abu 'Ubeid al-Qurashi, "Fourth Generation Wars," 28 January 2002.

Defining Terrorism

The Department of Defense approved definition of terrorism is: "The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."[25] For the purposes of this document, this will be the standard definition. However, this is not the last or only word on the subject. A researcher did a review of writings on terrorism and found 109 different definitions![26] Here is a sampling of definitions to illustrate the difficulties of categorizing and analyzing terrorism.

The FBI uses this: "Terrorism is the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[27] The U.S. Department of State uses the definition contained in Title 22 U.S.C. Section 2656f(d). According to this section, "terrorism" means "premeditated politically-motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience."[28] These definitions stress the respective institutional concerns of the organizations using them. The FBI concentrates on the "unlawful" aspect, in keeping with its law-enforcement mission. The Department of State concerns itself with "politically motivated" actions by "sub-national" or "clandestine" actors, a focus appropriate to the Department's functions of international relations and diplomacy.

Outside the United States Government, there are greater variations in what features of terrorism are emphasized in definitions. The United Nations produced this definition in 1992; "An anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby - in contrast to assassination - the direct targets of violence are not the main targets." The most commonly accepted academic definition starts with the U.N. definition quoted above, and adds two sentences totaling another 77 words on the end; containing such verbose concepts as "message generators" and 'violence based communication processes."[29] Less specific and considerably less verbose, the British Government definition of 1974 is "…the use of violence for political ends, and includes any use of violence for the purpose of putting the public, or any section of the public, in fear."[30]

Common Elements of Terrorism

There is clearly a wide choice of definitions for terrorism. Despite this, there are elements in common among the majority of useful definitions. Common threads of the various definitions identify terrorism as:

---

[25] FM 100-20, *Military Operations in Low Intensity Conflict*, 5 December 1990; and Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 09 January 2003.

[26] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 39.

[27] Title 28, Code of Federal Regulations, Section 0.85, *Judicial Administration*, (Washington, D.C., July 2001).

[28] Department of State, *Patterns of Global Terrorism 2001* (Washington, D.C., May 2002), xvi.

[29] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "The Academic View."

[30] Ibid., s.v. "The Official View."

- Political
- Psychological
- Violent
- Dynamic
- Deliberate

Political

A terrorist act is a political act or is committed with the intention to cause a political effect. Clausewitz' statement that "war is a continuation of policy by other means" is taken as a truism by terrorists. They merely eliminate the intermediate step of armies and warfare, and apply violence directly to the political contest.[31] Over a decade ago, a U.S. State Department official summarized, "The ultimate goals of terrorism are political…Politically motivated terrorism invariably involves a deeply held grievance over some form of injustice. The injustice may be social or economic, but it is nonetheless blamed on a political authority." [32]

Psychological

The intended results of terrorist acts cause a psychological effect ("terror"). They are aimed at a target audience other than the actual victims of the act. The intended target audience of the terrorist act may be the population as a whole, some specific portion of a society (an ethnic minority, for example similar to the situation in Kosovo between the Serbs and Albanians), or decision-making elites in the society's political, social, or military populace.

Violent

Violence, coercion, and destruction are used in the commission of the act to produce the desired effect. Even if casualties or destruction are not the result of a terrorist operation, the threat or potential of violence is what produces the intended effect. For example, a successful hostage taking operation may result in all hostages being freed unharmed after negotiations and bargaining. Regardless of the outcome, the terrorist bargaining chips were nothing less than the raw threat of applying violence to maim or kill some or all of the hostages. When the threat of violence is not credible, or the terrorists are unable to implement violence effectively, terrorism fails.

Dynamic

Terrorist groups demand change, revolution, or political movement. The radical worldview that justifies terrorism mandates drastic action to destroy or alter the status quo. Even if the goals of a movement are reactionary in nature, they require action to "turn back the clock" or restore some cherished value system that is extinct. Nobody commits violent attacks on strangers or innocents to keep things "just the way they are."

---

[31] Karl von Clausewitz, *War, Politics and Power* (Chicago: Regnery Gateway, 1962), 83.
[32] David E. Long, *The Anatomy of Terrorism* (New York: THE FREE PRESS, A Division of Macmillan, Inc., 1990), 4 and 5.

Deliberate

Terrorism is an activity planned and intended to achieve particular goals. It is a rationally employed, specifically selected tactic, and is not a random act.[33] Since the victims of terrorist violence are often of little import, with one being as good for the terrorists' purposes as another, victim or target selection can appear random or unprovoked. But the target will contain symbolic value or be capable of eliciting emotional response according to the terrorists' goals. Remember that the actual target of terrorism is not necessarily the victim of the violence, but the psychological impact on the society or population. This psychological impact is intended to create an environment of fear and intimidation that terrorists can then manipulate to force others to submit or agree to their demands.

Specific Observations

In addition to these common elements derived from attempts to define terrorism, some specific observations about terrorists become apparent. These observations are not definitive; meaning they do not automatically indicate terrorist activity. But they are common to the practice of terrorism.

Media Exploitation

As stated earlier, terrorism's effects are not necessarily aimed at the victims of terrorist violence. Victims are usually objects to be exploited by the terrorists for their effect on a third party. In order to produce this effect, information of the attack must reach the target audience. So any terrorist organization plans for exploitation of available media to get the message to the right audiences.[34] Victims are simply the first medium that transmits the psychological impact to the larger target audience. The next step in transmission will depend on what media is available, but it will be planned, and it will frequently be the responsibility of a specific organization within the terrorist group to do nothing else but exploit and control the news cycle.[35]

Some organizations can rely on friendly or sympathetic news outlets, but this is not necessary. News media can be manipulated by planning around the demands of the "news cycle," and the advantage that control of the initiative gives the terrorist. Pressures to report quickly, to "scoop" competitors, allow terrorists to present claims or make statements that might be refuted or critically commented on if time were available. Terrorists often provide names and details of individual victims to control the news media through its desire to humanize or personalize a story. For the victims of a terrorist attack, it is a certainty that the impact on the survivors (if there are any) is of minimal importance to the terrorists. What is important is the intended psychological impact that the news of their death or suffering will cause in a wider audience.

---

[33] Ehud Sprinzak, "Rational Fanatics," *Foreign Policy,* no. 120 (September/October 2000): 66-73.

[34] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 55-58.

[35] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 33.

Operations in Permissive Societies

Terrorists conduct more operations in societies where individual rights and civil legal protections prevail. While terrorists may base themselves in repressive regimes that are sympathetic to them, they usually avoid repressive governments when conducting operations wherever possible. An exception to this case is a repressive regime that does not have the means to enforce security measures. Governments with effective security forces and few guaranteed civil liberties have typically suffered much less from terrorism than liberal states with excellent security forces. Al Qaeda has shown, however, that they will conduct operations anywhere.

Illegality of Methods

Terrorism is a criminal act. Whether the terrorist chooses to identify himself with military terminology (as discussed under insurgencies below), or with civilian imagery (brotherhood, committee, etc.), he is a criminal in both spheres. The violations of civil criminal laws are self-evident in activities such as murder, arson, and kidnapping regardless of the legitimacy of the government enforcing the laws. Victimizing the innocent is criminal injustice under a dictatorship or a democracy.[36] If the terrorist claims that he is justified in using such violence as a military combatant, he is a de facto war criminal under international law and the military justice systems of most nations.

Preparation and Support

It is important to understand that actual terrorist operations are the result of extensive preparation and support operations. Media reporting and academic study have mainly focused on the terrorists' goals and actions, which is precisely what the terrorist intends. This neglects the vital but less exciting topic of preparation and support operations. Significant effort and coordination is required to finance group operations, procure or manufacture weapons, conduct target surveillance and analysis, and deliver trained terrorists to the operational area. While the time and effort expended by the terrorists may be a drop in the bucket compared to the amounts spent to defend against them, terrorist operations can still involve large amounts of money and groups of people. The need for dedicated support activities and resources on simple operations are significant, and get larger the greater the sophistication of the plan and the complexity of the target.

Differences between Terrorism and Insurgency

If no single definition of terrorism produces a precise, unambiguous description, the question can be approached by eliminating similar activities that are not terrorism, but that appear to overlap. For the U.S. military, two such related concepts probably lead to more confusion than others. Guerilla warfare and insurgencies are often assumed to be synonymous with terrorism. One reason for this is that insurgencies and terrorism often have similar goals.[37] However, if you examine insurgency and guerilla warfare, specific differences emerge.

---

[36] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 190.

[37] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Theories of Insurgency and Terrorism: Introduction."

A key difference is that an insurgency is a movement - a political effort with a specific aim. This sets it apart from both guerilla warfare and terrorism, as they are both methods available to pursue the goals of the political movement.

Another difference is the intent of the component activities and operations of insurgencies versus terrorism. There is nothing inherent in either insurgency or guerrilla warfare that requires the use of terror. While some of the more successful insurgencies and guerilla campaigns employed terrorism, and some developed into conflicts where use of terror tactics and terrorism became predominant; there have been others that effectively renounced the use of terrorism. The deliberate choice to use terrorism considers its effectiveness in inspiring further resistance, destroying government efficiency, and mobilizing support.[38] Although there are places where terrorism, guerilla warfare, and criminal behavior all overlap, groups that are exclusively terrorist, or subordinate "wings" of insurgencies formed to specifically employ terror tactics, usually demonstrate differences in their objectives and operations. Disagreement on the costs of using terror tactics, or whether terror operations are to be given primacy within the insurgency campaign, have frequently led to the "urban guerilla" or terrorist wings of an insurgency splintering off to pursue the revolutionary goal by their own methods.

> **Insurgency**: (JP 1-02)(NATO) An organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict.
>
> **Guerrilla Warfare**: (JP1-02) (NATO) Military and para-military operations conducted in enemy-held or hostile territory by irregular, predominantly indigen-ous forces.

The ultimate goal of an insurgency is to challenge the existing government for control of all or a portion of its territory, or force political concessions in sharing political power. Insurgencies require the active or tacit support of some portion of the population involved. External support, recognition or approval from other countries or political entities can be useful to insurgents, but is not required. A terror group does not require[39] and rarely has the active support or even the sympathy of a large fraction of the population. While insurgents will frequently describe themselves as "insurgents" or "guerrillas," terrorists will not refer to themselves as "terrorists" but describe themselves using military or political terminology ("freedom fighters," "soldiers," "activists"). Terrorism relies on public impact, and is therefore conscious of the advantage of avoiding the negative connotations of the term "terrorists" in identifying themselves.[40]

Aside from variations in definitions, real-world events can present situations that are vague and open to multiple interpretations. A common view of al Qaeda is that they are a transnational terrorist group. Correspondingly, al Qaeda could be defined as a global insurgency set to overthrow the current world order in regard to global economic systems and globalization. Al Qaeda does have political objectives of removing the

---

[38] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 16-20.
[39] Ibid., 17.
[40] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 29-33.

U.S. from the Middle East to enhance their ability to overthrow "apostate" moderate Arab regimes, such as the Saudi Arabia ruling family. A long-term vision would reconstitute the Caliphate. Using this religious power and the wealth of oil reserves and production, the new Caliphate could serve as a means of further spreading a form of Islam throughout the world.

On a regional perspective, the *Montoneros* of Argentina during the 1970s provide an example of tenuous distinctions between terrorism and guerrilla warfare. Incidents of kidnapping high profile businessmen for ransom or assassination of government officials blurred a widening array of terrorist actions that eventually presented organized military-type operations. Cellular and compartmented groups gave way to organized unit-type structure for sophisticated attacks against military forces. One attack against an infantry regiment included *Montoneros* marshalling their force over 800 kilometers from previous urban enclaves, forming assault and support elements, conducting the attack, evacuating the force with a hijacked airplane, providing medical treatment enroute to the dispersal landing field, and vanishing among the population after landing.[41]

Terrorism does not usually attempt to challenge government forces directly, but acts to change perceptions as to the effectiveness or legitimacy of the government itself. This is done by ensuring the widest possible knowledge of the acts of terrorist violence among the target audience. Rarely will terrorists attempt to "control" terrain, as it ties them to identifiable locations and reduces their mobility and security. Terrorists as a rule avoid direct confrontations with government forces. A guerilla force may have something to gain from a clash with a government combat force, such as proving that they can effectively challenge the military effectiveness of the government. A terrorist group has nothing to gain from such a clash. This is not to say that they do not target military or security forces, but that they will not engage in anything resembling a "fair fight," or even a "fight" at all. Terrorists use methods that neutralize the strengths of conventional forces. Bombings and mortar attacks on civilian targets where military or security personnel spend off-duty time, ambushes of undefended convoys, and assassinations of poorly protected individuals are common tactics. All of these actions were evident in terrorist operations in Iraq during 2003-2004.

> **"We have the right to kill four million Americans – two million of them children."**
>
> Suleiman abu Ghaith
> Al Qaeda Spokeman

Insurgency need not require the targeting of noncombatants, although many insurgencies expand the accepted legal definition of combatants to include police and security personnel in addition to the military. Terrorists usually do not discriminate between combatants and noncombatants, or if they do, they broaden the category of "combatants" so much as to render it meaningless. Deliberate dehumanization and criminalization of the enemy in the terrorists' mind justifies extreme measures against anyone identified as hostile (more on this in Chapter 2). Terrorists often expand their groups of acceptable targets, and conduct operations against new targets without any warning or notice of hostilities.

---

[41] Alan C. Lowe, "Todo o Nada: Montonerosa Versus the Army: Urban Terrorism in Argentina," ed. William G. Robertson and Lawrence A. Yates, in *Block by Block: The Challenges of Urban Operations* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2003), 392-396.

Ultimately, the difference between insurgency and terrorism comes down to the intent of the actor. Insurgency movements and guerilla forces can adhere to international norms regarding the law of war in achieving their goals, but terrorists are by definition conducting crimes under both civil and military legal codes. Terrorists routinely claim that were they to adhere to any "law of war" or accept any constraints on the scope of their violence, it would place them at a disadvantage vis-à-vis the establishment. Since the nature of the terrorist mindset is absolutist, their goals are of paramount importance, and any limitations on a terrorist's means to prosecute the struggle are unacceptable.[42]

Use of Terror by Nation-States: Is There a Difference?

Is there a difference between terrorism and the use of specific tactics that exploit fear and terror by authorities normally considered "legitimate"? Nations and states often resort to violence to influence segments of their population, or rely on coercive aspects of state institutions. Just like the idea of equating any act of military force with terrorism described above, there are those who equate any use of government power or authority versus any part of the population as terrorism. This view also blurs the lines of what is and is not terrorism, as it elevates outcomes over intentions. Suppression of a riot by law enforcement personnel may in fact expose some of the population (the rioters) to violence and fear, but with the intent to protect the larger civil order. On the other hand, abuse of the prerogative of legitimized violence by the authorities is a crime.

However, there are times when national governments will become involved in terrorism or utilize terror to accomplish the objectives of governments or individual rulers. Most often, terrorism is equated with "non-state actors," or groups that are not responsible to a sovereign government. However, internal security forces can use terror to aid in repressing dissent, and intelligence or military organizations perform acts of terror designed to further a state's policy or diplomatic efforts abroad.

A government that is an adversary of the United States may apply terror tactics in an effort to add depth to their engagement of U.S. forces. Repression through terror of the indigenous population would take place to prevent internal dissent and insurrection that the U.S. might exploit. Military special operations assets and state intelligence operatives could conduct terrorist operations against U.S. interests both in theater and as far abroad as their capabilities allow. Finally, attacks against the U.S. homeland could be executed by state sponsored terrorist organizations or by paid domestic proxies. Three different ways that states can engage in the use of terror are:

- Governmental or "State" terror

- State involvement in terror

- State sponsorship of terrorism

Governmental or "State" Terror: This is sometimes referred to as "terror from above," where a government terrorizes its own population to control or repress them. These actions usually

---

[42] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 33.

constitute the acknowledged policy of the government, and make use of official institutions such as the judiciary, police, military, and other government agencies. Changes to legal codes permit or encourage torture, killing, or property destruction in pursuit of government policy. After assuming power, official Nazi policy was aimed at the deliberate destruction of "state enemies" and the resulting intimidation of the rest of the population. Stalin's "purges" of the 1930s are examples of using the machinery of the state to terrorize a population. The methods he used included such actions as rigged show trials of opponents, punishing family or friends of suspected enemies of the regime, and extra-legal use of police or military force against the population.[43]

Saddam Hussein used chemical weapons on his own Kurdish population without any particular change or expansion of policies regarding the use of force on his own citizens. They were simply used in an act of governmental terror believed to be expedient in accomplishing Hussein's goals.

State Involvement in Terror: These are activities where government personnel carry out operations using terror tactics. These activities may be directed against other nations' interests, its own population, or private groups or individuals viewed as dangerous to the state. In many cases, these activities are terrorism under official sanction, although such authorization is rarely acknowledged openly. Historical examples include the Soviet and Iranian assassination campaigns against dissidents who had fled abroad, and Libyan and North Korean intelligence operatives downing airliners on international flights.[44]

Other types of these activities are "death squads" or "war veterans": unofficial actions taken by officials or functionaries of a regime (such as members of police or intelligence organizations) to repress or intimidate their own population. While these officials will not claim such activities, and disguise their participation, it is often made clear that they are acting for the state. Keeping such activities "unofficial" permits the authorities deniability and avoids the necessity of changing legal and judicial processes to justify oppression. This is different than "pro-state" terror, which is conducted by groups or persons with no official standing and without official encouragement. While pro-state terror may result in positive outcomes for the authorities, their employment of criminal methods and lack of official standing can result in disavowal and punishment of the terrorists, depending on the morality of the regime in question.

State Sponsorship of Terrorism: These activities occur when governments provide supplies, training, and other forms of support to non-state terrorist organizations. This type affiliation can be state-sponsored or state-directed, as discussed in Chapter 3. One of the most valuable types of this support is the provision of safe haven or physical basing for the terrorists' organization. Another crucial service a state sponsor can provide is false documentation, not only for personal identification (passports, internal identification documents), but also for financial transactions and weapons purchases. Other means of support are access to training facilities and expertise not readily available to groups without extensive resources. Finally, the extension of diplomatic protections and services, such as immunity from extradition, diplomatic passports, use of embassies and other protected grounds, and diplomatic pouches to transport weapons or explosives have been significant to some groups.

---

[43] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Stalin's Great Terror."
[44] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 190.

An example of state sponsorship is the Syrian government's support of HAMAS and Hizballah in Lebanon. Syrian resources and protection enable the huge training establishments in the Bek'aa Valley. On a smaller, more discreet scale, the East German Stasi provided support and safe-haven to members of the Red Army Faction (RAF or Baader Meinhof Gang) and neo-fascist groups that operated in West Germany.[45] Wanted members of the RAF were found resident in East Germany after the fall of the Berlin Wall in 1989.

Section II: Historical Overview of Terrorism

U.S. forces need to be aware that there is a historical perspective to terrorism and that terrorists have directly targeted military personnel and facilities since the earliest times. In the 1980s, European and American radical Left terror groups targeted significant numbers of U.S. service members.[46] Now, greater involvement of U.S. military forces in terrorist related operations, either as targets or combatants, makes attacks on military personnel and facilities more likely than in the past.

Terror in Antiquity: First to Fourteenth Century A.D.

The earliest known organization that exhibited aspects of a modern terrorist organization was the Zealots of Judea. Known to the Romans as *sicarii*, or dagger-men,[47] they carried on an underground campaign of assassination of Roman occupation forces, as well as any Jews they felt had collaborated with the Romans. Their motive was an uncompromising belief that they could not remain faithful to the dictates of Judaism while living as Roman subjects. Eventually, the Zealot revolt became open, and they were finally besieged and committed mass suicide at the fortification of Masada.

The Assassins were the next group to show recognizable characteristics of terrorism, as we know it today. A breakaway faction of Shia Islam called the Nizari Ismalis adopted the tactic of assassination of enemy leaders because the cult's limited manpower prevented open combat.[48] Their leader, Hassam-I Sabbah, based the cult in the mountains of Northern Iran. Their tactic of sending a lone assassin to successfully kill a key enemy leader at the certain sacrifice of his own life (the killers waited next to their victims to be killed or captured) inspired fearful awe in their enemies.

> The word "Assassin" was brought back to Europe by the Crusaders, and refers to the widespread rumor that the Nizari used hashish to produce the fanatical courage their lone knife-wielding killers repeatedly demonstrated.

Even though both the Zealots and the Assassins operated in antiquity, they are relevant today: First as forerunners

---

[45] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 200.

[46] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Chronology of Terrorist Events."

[47] Franklin L. Ford, *Political Murder: From Tyrannicide to Terrorism* (Cambridge: Harvard University Press, 1985), 91.

[48] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "The Assassins: A Terror Cult."

of modern terrorists in aspects of motivation, organization, targeting, and goals. Secondly, although both were ultimate failures, the fact that they are remembered hundreds of years later, demonstrates the deep psychological impact they caused.

Early Origins of Terrorism: Fourteenth to Eighteenth Century

From the time of the Assassins (late 13th century) to the 1700s, terror and barbarism were widely used in warfare and conflict,[49] but key ingredients for terrorism were lacking. Until the rise of the modern nation state after the Treaty of Westphalia in 1648, the sort of central authority and cohesive society that terrorism attempts to influence barely existed. Communications were inadequate and controlled, and the causes that might inspire terrorism (religious schism, insurrection, ethnic strife) typically led to open warfare. By the time kingdoms and principalities became nations, they had sufficient means to enforce their authority and suppress activities such as terrorism.

The French Revolution provided the first uses of the words "Terrorist" and "Terrorism." Use of the word "terrorism" began in 1795 in reference to the Reign of Terror initiated by the Revolutionary government. The agents of the Committee of Public Safety and the National Convention that enforced the policies of "The Terror" were referred to as "Terrorists." The French Revolution provided an example to future states in oppressing their populations. It also inspired a reaction by royalists and other opponents of the Revolution who employed terrorist tactics such as assassination and intimidation in resistance to the Revolutionary agents.[50] The Parisian mobs played a critical role at key points before, during, and after the Revolution. Such extra-legal activities as killing prominent officials and aristocrats in gruesome spectacles started long before the guillotine was first used.[51]

Entering the Modern Era: The Nineteenth Century

During the late nineteenth century, radical political theories and improvements in weapons technology spurred the formation of small groups of revolutionaries who effectively attacked nation-states. Anarchists espousing belief in the "propaganda of the deed" produced some striking successes, assassinating heads of state from Russia, France, Spain, Italy, and the United States. However, their lack of organization and refusal to cooperate with other social movements in political efforts rendered anarchists ineffective as a political

> **"Propaganda of the Deed"**
> "Acts of revolution, resistance, or violence that will inspire the masses to act. It assumes that there is an untapped force of revolutionary will in the population at large."

movement. In contrast, Communism's role as an ideological basis for political terrorism was just beginning, and would become much more significant in the twentieth century.

Another trend in the late nineteenth century was the increasing tide of nationalism throughout Europe, in which the nation (the identity of a people) and the political state were combined. As states began to emphasize national identities, peoples that had been conquered or

---

[49] Caleb Carr, *The Lessons of Terror: A History of Warfare Against Civilians: Why it has Always Failed and Why it will Fail Again* (New York: Random House, 2002), 52-63.
[50] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Terror in the French Revolution 1789-1815."
[51] Simon Schama, *Citizens: A Chronicle of The French Revolution* (New York: Alfred A. Knopf, Inc., 1989), 405 & 447.

colonized could, like the Jews at the times of the Zealots, opt for assimilation or struggle.

The best-known nationalist conflict from this time is still unresolved − the multi-century struggle of Irish nationalism. Nationalism, like communism, became a much greater worldwide and ideological force in the twentieth century.

The terrorist group from this period that serves as a model in many ways for what was to come was the Russian Narodnya Volya (Peoples Will).[52] This group displayed many of the traits of terrorism organization and conduct: clandestine, cellular, impatient and unable to organize the constituents they claimed to represent; and a tendency to increase the level of violence as pressures on the group mounted. However, they would sometimes call off attacks that might endanger individuals other than their intended target. Today, there are still many terrorist organizations that attempt to prevent collateral casualties in their operations. Unfortunately, many terrorist organizations appear to use indiscriminate levels of violence as an effective technique to achieve notoriety and media attention.

The Early Twentieth Century

The first half of the twentieth century saw two events that influenced the nature of conflict to the present day. The effects of two World Wars inflamed passions and hopes of nationalists throughout the world, and severely damaged the legitimacy of international order and governments.

Damaged Legitimacy

The "total war" practices of all combatants of WWII provided further justification for the "everybody does it" view of the use of terror and violations of the law of war. The desensitization of people and communities to violence that started in World War I accelerated during World War II. The intensity of the conflict between starkly opposed ideologies led to excesses on the part of all participants. New weapons and strategies that targeted the enemies' civilian population to destroy their economic capacity for conflict exposed virtually every civilian to the hazards of combatants. The major powers' support of partisan and resistance organizations using terrorist tactics was viewed as an acceptance of their legitimacy. It seemed that civilians had become legitimate targets, despite any rules forbidding it.[53]

Nationalism on the Rise

Nationalism intensified during the mid to late twentieth century throughout the world. It became an especially powerful force in the subject peoples of various colonial empires. Although dissent and resistance were common in many colonial possessions, results could be achieved sometimes through dedicated nonviolence, such as in India. Other examples against colonialism witnessed terrorism as a specific program of nationalist movements. In open warfare, nationalist identities became a focal point for these actions.

Gradually, as nations became closely tied to concepts of race and ethnicity, international political developments began to support such concepts. Members of ethnic groups whose states had been absorbed by others or had ceased to exist as separate nations saw

---

[52] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Russian Anarchist Terror."
[53] Martin L. Van Creveld, *The Transformation of War* (New York: The Free Press, 1991), 79.

opportunities to realize nationalist ambitions. Several of these groups chose terror as a method to conduct their struggle and make their situation known to world powers they hoped would be sympathetic. In Europe, both the Irish and the Macedonians had existing terrorist campaigns as part of their ongoing struggle for independence, but had to initiate bloody uprisings to further their cause. The Irish were partially successful, the Macedonians failed.

The Later Twentieth Century

Cold War Developments

The bi-polar world of the Cold War changed perception of conflicts the world over. Relatively minor confrontations took on significance as arenas where the superpowers could compete without risking escalation to full nuclear war. Conflict in the form of "proxy wars" between the East and the West took place on the peripheries, and was limited in scope to prevent escalation. During the immediate postwar period, terrorism was more of a tactical choice by leaders of nationalist insurgencies and revolutions. Successful campaigns for independence from colonial rule occurred throughout the world, and many employed terrorism as a supporting tactic. When terrorism was used, it was used within the framework of larger movements, and coordinated with political, social, and military action. Even when terrorism came to dominate other aspects of a nationalist struggle, such as the Palestinian campaign against Israel, or the Jewish campaign against the British, psychological stress and eroding an opponent's resolve remained significant objectives in support of principal aims.

Throughout the Cold War, the Soviet Union provided direct and indirect assistance to revolutionary movements around the world. Many anti-colonial movements found the revolutionary extremism of communism attractive. Leaders of these "wars of national liberation" saw the advantage of free weapons and training. They also realized that the assistance and patronage of the Eastern Bloc meant increased international legitimacy. Many of these organizations and individuals utilized terrorism in support of their political and military objectives. The policy of the Soviet Union to support revolutionary struggles everywhere, and to export revolution to non-communist countries, provided extremists willing to employ violence and terror as the means to realize their ambitions.

The Internationalization of Terror

The age of modern terrorism might be said to have begun in 1968 when the Popular Front for the Liberation of Palestine (PFLP) hijacked an El Al airliner en route from Tel Aviv to Rome. While hijackings of airliners had occurred before, this was the first time that the nationality of the carrier (Israeli) and its symbolic value was a specific operational aim. Also a first was the deliberate use of the passengers as hostages for demands made publicly against the Israeli government. The combination of these unique events, added to the international scope of the operation, gained significant media attention. The founder of PFLP, Dr. George Habash observed that the level of coverage was tremendously greater than battles with Israeli soldiers in their previous area of operations. In a 1970 interview, Habash stated that although his cause did not receive much media coverage prior to the highjacking, "At least the world is talking about us now."[54] Following the El Al highjacking, international

---

[54] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 70.

real-time notoriety became more the norm. The 1970 PFLP destruction of a passenger aircraft, with passengers already removed, was presented on live international television. However, probably the most well known terrorist incident that propelled a cause from obscurity to the international stage was the murder of Israeli athletes by Palestinian terrorists during the Munich Olympics in 1972.

Another aspect of this internationalization is the cooperation between extremist organizations in conducting terrorist operations. Cooperative training between Palestinian groups and European radicals started as early as 1970, and joint operations between the PFLP and the Japanese Red Army (JRA) began in 1974. Since then international terrorist cooperation in training, operations, and support has continued to grow, and continues to this day. Motives range from the ideological, such as the 1980s alliance of the Western European Marxist-oriented groups, to financial, as when the IRA exported its expertise in bomb making as far reaching as Colombia.

To highlight the true international nature of terrorism, Chart 1-1 depicts the number of international terrorist incidents by region for 1997 through 2003, and Chart 1-2 shows the number of casualties by region over the same timeframe.[55]

Chart 1-1: International Terrorist Incidents by Region 1997 - 2003

---
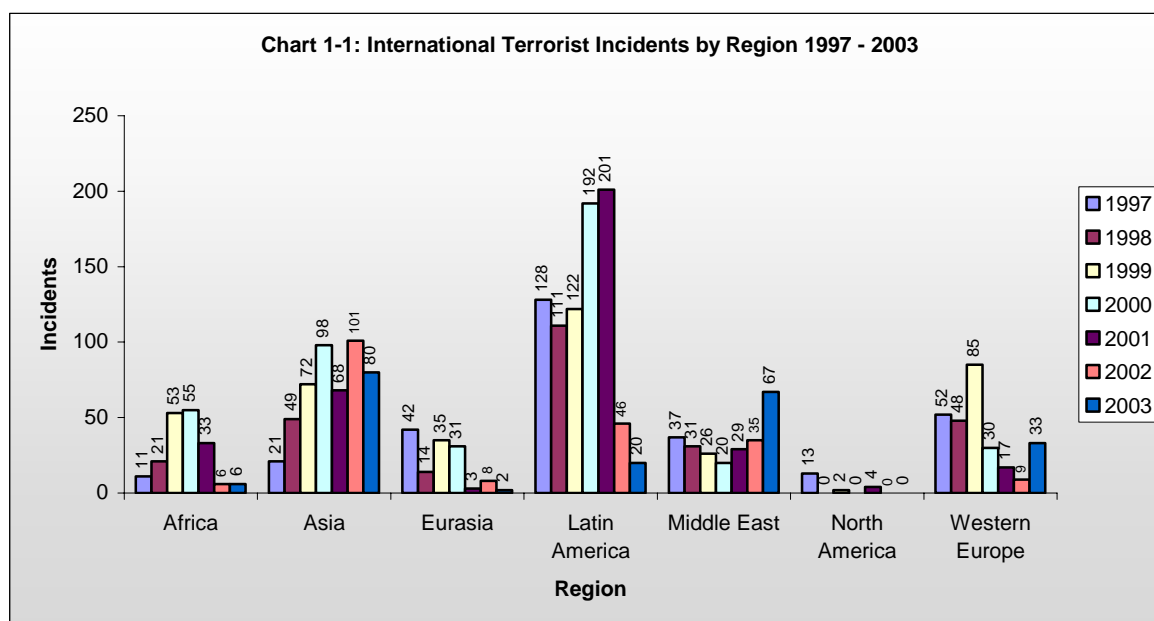
[55] Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2003* (Washington, D.C., April 2004, revised 22 June 2004), 177-178; and *Patterns of Global Terrorism 2002* (Washington, D.C., April 2003), 162-163.

Chart 1-2: Total International Casualties by Region 1997 - 2003

Casualties (y-axis: 0 to 6000)

Legend: 1997, 1998, 1999, 2000, 2001, 2002, 2003

Africa: 28, 5379, 185, 102, 150, 67, 14
Asia: 344, 635, 690, 904, 651, 1283, 1427
Eurasia: 27, 12, 8, 103, 0, 615, 0
Latin America: 11, 195, 20, 7, 54, 79
Middle East: 480, 68, 31, 78, 513, 1047, 1823
North America: 7, 0, 0, 0, 4465, 0, 0
Western Europe: 17, 405, 6, 5, 20, 6, 928

Region
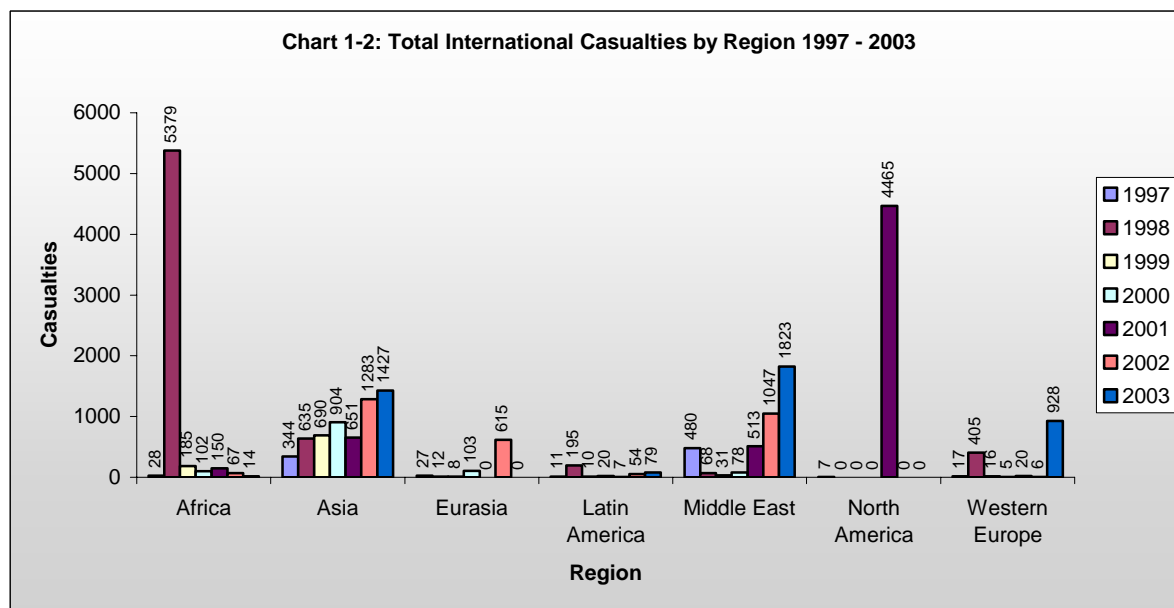
This internationalization of terrorism has had a direct impact on the United States. Figures 1-1 through 1-4 reflect what the U.S. Department of State, Bureau of Public Affairs considers significant terrorist incidents from 1970 through the end of 2003. As you can see, there were 16 significant events in the decade of the 1970s, with 9 of those events involving the United States or its citizens in some fashion. The decade of the 1990s shows an increase in total incidents of nearly 500% over that of the 1970s, and an increase of 644% in incidents involving the United States. In just the first four years of the decade of the 2000s, there was an increase of 750% over that of the 1970s in overall terrorist incidents, and an increase of 411% in incidents involving the United States. [56] (Incidents in red/*italics* involve the U.S.)

Total Events = 16   U.S. Involved = 9

Timeline (1970–1980):

July 1970 USAID Adviser Kidnapped & Killed in Uruguay
July 1972 "Bloody Firday" IRA attack in Belfast
September 1972 Munich Olympic Massacre
March 1973 US Ambassador Assassinated in Sudan
May 1973 US Consul General Kidnapped in Mexico
January 1975 Wall Street Bombing
June 1976 Entebbe Hostage Crisis in Uganda
March 1978 Italian Prime Minister Kidnapped & Assassinated
February 1979 US Ambassador to Afghanistan Assassinated
November 1979 Grand Mosque Seizure in Saudi Arabia

February 1970 Attack on Munich Airport
December 1973 Attack on Rome Airport
August 1974 US Ambassador to Cyprus Assassinated
January 1975 US State Dept Bombed
September 1976 Chilean Foreign Minister Killed in Washington
November 1979 US Embassy Seized in Iran

Figure 1-1: **Significant Terrorist Incidents 1970 through 1979**
Source: U.S. Department of State, Office of the Historian, Bureau of Public Affairs, March 2004

---

[56] Department of State, Office of the Historian, Bureau of Public Affairs, *Significant Terrorist Incidents, 1961-2003: A Brief Chronology* (Washington, D.C., March 2004), 1-19; available from http://www.state.gov/r/pa/ho/pubs/fs/5902pf.htm; Internet; accessed 19 April 2004.

Total Events = 37   U.S. Involved = 23

April 1984 Bombing of US Servicemen in Torrejon, Spain

June 1985 Air India Bombing

June 1985 FMLN Attack in El Salvador

September 1986 Kimpo Airport Bombing in Seoul

October 1983 South Korean Delegation Bombed in Rangoon

October 1984 Prime Minister Gandhi Assassinated in India

November 1985 Egyptian Airline Hijacking in Athens

December 1987 Servicemen's Bar Bombing in Barcelona

September 1982 Lebanese Prime Minister Assassinated in Beirut

November 1983 US Naval Officer Assassinated in Greece

June 1988 US Defense Attache Killed in Greece

December 1981 US Missionaries Murdered in El Salvador

April 1983 US Embassy Bombed in Beirut

June 1985 TWA Hijacking in Rome

April 1986 Berlin Discoteque Bombing in Germany

April 1987 Bus Bombing in Athens

April 1988 USO Bombing in Naples

April 1989 US Army Officer Killed in Manila

August 1981 Ramstein AB Bombed in Germany

1980   1981   1982   1983   1984   1985   1986   1987   1988   1989   1990

April 1983 US Citizen Kidnapped in Colombia

October 1983 Marine & French Barracks Bombed in Beirut

February 1985 DEA Agents Kidnapped & Killed in Mexico

March 1986 TWA Bombing in Athens

November 1987 Korean Airlines Bombing over Indian Ocean

February 1988 USMC Officer Kidnapped and Murdered in Lebanon

September 1989 UTA Flight Bombing over Niger

October 1981 President Sadat Assassinated in Egypt

June 1984 Golden Temple Seizure in Amritsar, India

May 1983 US Naval Officer Assassinated in El Salvador

September 1985 Soviet Diplomats Kidnapped in Beirut

December 1985 Airport Attacks in Rome and Vienna

December 1988 PanAm 103 Bombing over Lockerbie, Scotland

November 1989 German Bank Chairman Assassinated in Frankfurt

March 1984 US Embassy Official Kidnapped & Murdered in Beirut

October 1985 Achille Lauro Hijacking in the Mediterranean Sea

Figure 1-2: **Significant Terrorist Incidents 1980 through 1989**
Source: U.S. Department of State, Office of the Historian, Bureau of Public Affairs, March 2004

Total Events = 79   U.S. Involved = 58

March 1992 Israeli Embassy Bombed in Argentina

April 1993 Attempted Assassination of President Bush in Kuwait

December 1994 Air France Hijacking in Algeria

February 1999 Greek Embassy Seizure in Vienna

March 1999 US Citizens & Others Kidnapped & Killed in Uganda

January 1990 US Embassy Bombed in Peru

January 1991 Attempted Bombing of US Ambassador to Indonesia

January 1992 US Businessmen Kidnapped in Philippines

January 1993 US Missionaries Kidnapped in Colombia

February 1994 Massacre of Moslems in Hebron

January 1999 UN Plane Shot Down in Angola

June 1999 Bombing of Shell Oil Platform in Nigeria

October 1999 Burmese Embassy Seizure in Bangkok

December 1999 US Citizen Kidnapped in Colombia

1990   1991   1992   1993   1994   1995   1999   2000

May 1990 US Air Force Personnel Killed in Philippines

January 1991 Attempted Bombing at USIS Library in Manila

January 1992 US Businessmen Kidnapped in Colombia

February 1993 World Trade Center Bombing in New York

September 1994 US Citizen Kidnapped in Colombia

February 1999 Pipe Bomb Attack in Uganda

March 1999 US Citizen Kidnapped in Colombia

August 1999 Kidnapping of UN Personnel in Sierra Leone

December 1999 Indian Airlines Hijacking in Kathmandu

February 1999 US Citizens Kidnapped & Killed in Venezuela

Figure 1-3: **Significant Terrorist Incidents 1990 through 1999**
Source: U.S. Department of State, Office of the Historian, Bureau of Public Affairs, March 2004

1-17

Total Events = 120   U.S. Involved = 37

Figure 1-4: **Significant Terrorist Incidents 2000 through 2003**
Source: U.S. Department of State, Office of the Historian,Bureau of Public Affairs, March 2004

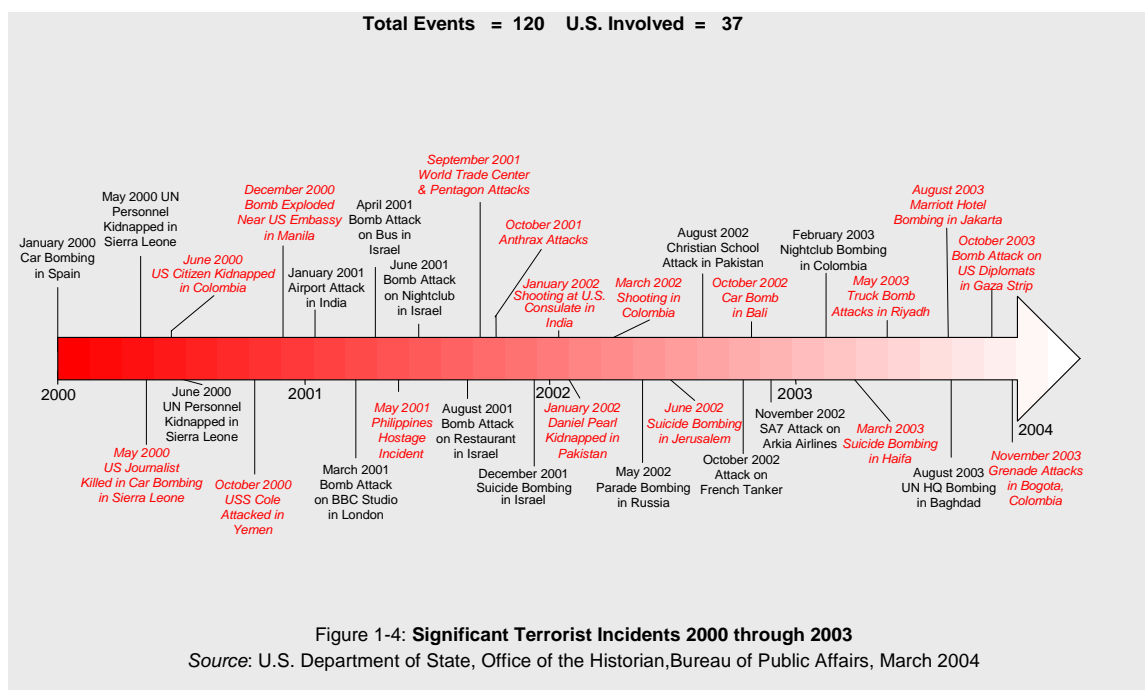Chart 1-3 consolidates the data from Figures 1-1 through 1-4 and reflects the growing trend of terrorist incidents since the 1970s. If you project out the actual statistics for the first 4 years of the decade of the 2000s to the end of December 2009, the total number of terrorist incidents for this first decade of the twenty-first century would be 300, with 92 of them involving the United States.
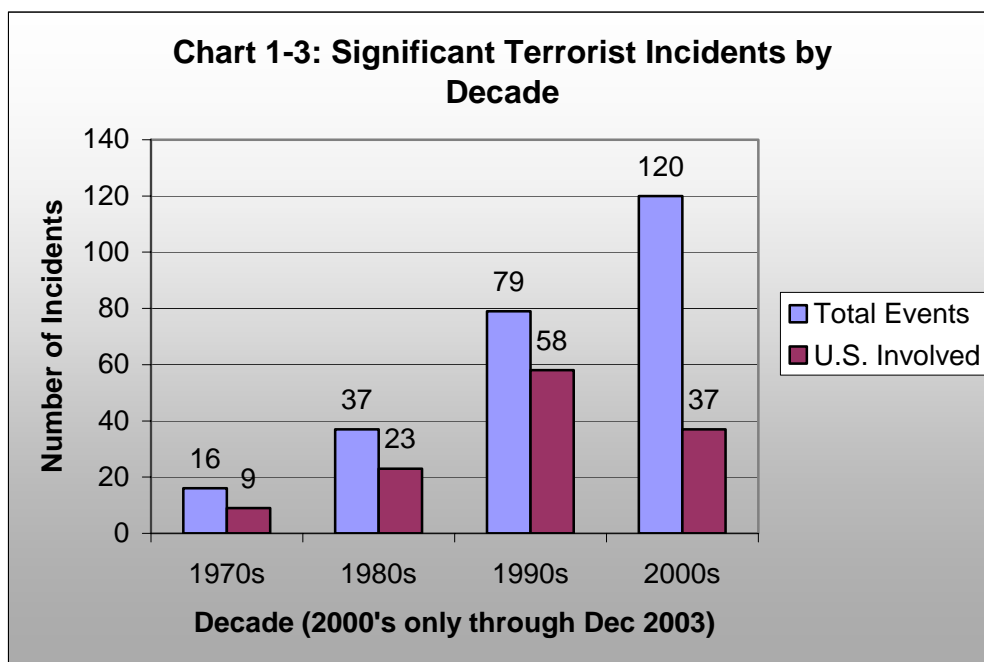
State Sponsorship of Terrorism

State sponsorship of the use of terror is not a strictly modern occurrence. Serbian intelligence officers provided support to the assassins who killed Arch Duke Franz Ferdinand of Austria, and precipitated World War I.[57] Germany provided arms to Irish nationalists during that war to use against the British.[58] Since then, state assistance to terrorists was used both as a means of surrogate warfare between states, and also as an international diplomatic tool. State sponsorship renders terrorism decidedly more effective. Access to a government's resources of weapons, information, money, and expertise, and use of its privileges in diplomatic travel, transportation, and protection made identifiable state sponsored acts eight times as lethal in the 1980s than non-state attacks. State sponsorship also increases lethality by reducing the need for support from constituent populations, leaving the terrorist free to operate without fear of backlash due to excessive violence.[59] The low cost and deniability of this technique has led to its adoption by nations with ambitious foreign policy goals and limited means.

During the 1970s and 1980s, the Soviet Union provided significant assistance to a wide variety of organizations and individuals involved in terrorism. Attempts to destabilize governments through the use of sponsored terrorist groups to some extent replaced "wars of national liberation" as a method of the Soviet Union during this period.[60] Although the USSR officially denounced terrorism, it provided support directly and via surrogates. Commonly, training in revolutionary theory and practical skills were provided to promising individuals from other countries, some of whom the KGB or GRU recruited for intelligence service. Safe havens were provided for members of terrorist groups in East bloc countries such as East Germany and Czechoslovakia. Weapons and explosives were given to radical regimes such as Libya, with the knowledge that they would likely end up in the hands of terrorist groups.

The example provided by the Soviet experience led other countries to adopt state sponsorship. Ranging from tenuous diplomatic support internationally, to direct operational control of a terrorist organization, state involvement in terror can be a flexible, low-risk tool for a variety of policy goals. Iran in particular has found sponsorship of terror to particularly suit its objective of militant Islamic revolution. The incidence of state sponsorship declined somewhat after the collapse of the Soviet Union due to isolation and retaliation on other identified state sponsors. However, this type of support shows no signs of completely going away.

Current State of Terrorism

Currently terrorism continues its process of evolution. Although future trends in terrorism will be covered at length in Chapter 6, we are seeing the beginning of many of those trends in current conditions. Shifts in the dominant motivations for terrorists; changes in organizational structures; and the changes in response to world developments such as the global economy and the development of information technology have altered considerably the nature of terrorism.

---

[57] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Assassination at Sarajevo 1914."

[58] Ibid., s.v. "State Sponsored Terrorism."

[59] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 189.

[60] Uri Ra'anan, ed., et al*., Hydra of Carnage; International Linkages of Terrorism* (Lexington: Lexington Books, 1986), 11.

Changes in Dominant Ideologies

Religious ideology has replaced political and nationalist ideologies as a principal cause for terrorist groups. The critical assessments of communism after the failure of the USSR caused a specific depreciation of leftist ideologies. One practical reason was the absence of major funding from the USSR for such leftist movements. Although political and nationalist rationales still exist, religious and right wing ideologies have gained more support in recent decades. To cite one example, international terrorist groups espousing religious ideologies went from three percent of total international terror groups in 1980, to forty six percent of international groups by 1995.[61] And the trend is accelerating. Also, the emergence of "single issue" movements, limited to a single concern such as environmentalism or anti-globalization, has started to supplant revolutionary ideology.

For many of the social revolutionaries, the failure of the Soviet Union, and of virtually all of the Eastern bloc communist governments, severely discredited Marxist-Leninist ideologies. The loss of supportive governments also impacted the viability of the left-wing groups in Europe. Also, nationalist movements that might have previously turned to terrorism have had success in realizing their goals in the post Cold War world. A large number of separatist movements were accorded international recognition and acceptance as the old world order shifted. Although in some areas, such as the former Yugoslavia, this process has been anything but peaceful, it has not seen long campaigns of insurgent warfare and terrorism previously associated with nationalist struggles.

Changes to Organizational Structures

In response to improvements in counter-terror capabilities, and increased cooperation between governments, terrorist groups are moving to networked organizational models, rather than hierarchical structures. Similar to the "leaderless resistance" model of the American right wing and "eco-terror" domestic groups, this decentralized organization takes advantage of uniform ideology or beliefs to guide the efforts toward the group's goals. The huge advances made in personal communication and privacy technology have enabled this change to a networked organization. It will be discussed in Chapter 3, but features:

- Increased security, due to fewer communications, no identifiable leadership or command structures, and less required coordination between elements not directly involved in operations.

- Faster response cycles to new countermeasures and tactics.

- Increased deniability, as actions can be acknowledged or disavowed depending on the results.

Changes to Global Conditions

Information technology has provided significant increases to the operational capabilities of terrorists, and also tightened the symbiotic relationship between terrorism and the media. The spread of information technology together with the rise of globalization has enhanced the

---

[61] Bruce Hoffman, *Inside Terrorism* (New York: Columbia Universalty Press, 1998), 90.

terrorist capability to communicate, collect intelligence, operate and spread its message. Terror tactics have expanded in scope, and increased in effectiveness in proportion to the development of global media and information technology. The transmission of the message has likewise become easier and more amenable to manipulation by the terrorist.

Today, terrorists are organizing themselves in more fluid ad hoc amalgamations of individuals who appear to have been brought together for a specific, "one time only" mission. Fewer barriers between countries for people and finances are intended to improve commerce, global trade, and freedom of movement, but are enabling factors for modern terrorists and contribute to the development of ad hoc, limited duration alliances and relationships.[62] These terrorist groups may emerge from obscurity to strike, and then just as suddenly disappear.

Terrorism historically flourishes in areas that are permissive. The presence in the modern world of failed states, or dysfunctional governments, has given the terrorist a replacement for state sponsorship, with few of the disadvantages. Weak governments attract criminal activity and outcast movements. Terrorist organizations, such as Hizballah in southern Lebanon, build popular support by providing services to the local population. In this developing relationship, terror organizations can become local power brokers, commanding more money and technical expertise than the "legitimate" government. In return for assistance from the terrorists, the government provides physical refuge and the protection the status of a sovereign government provides against retaliation and arrest.

U.S. Legal Status of Terrorist Organizations

Within the global community, there are legal categories that define terrorist organizations according to legal statutes or in relation to national or international laws. Legal categories usually define a state's or group of states' relation to the terrorist organization. Such a relationship may range from toleration of activities that do no harm to the state in question to proscribing membership or support of such an organization as a criminal act. In the United States, two particular legal categories are:

- DFTO (Designated Foreign Terrorist Organization); this is a political designation determined by the U.S. Department of State. Listing as a DFTO imposes legal penalties for membership, prevents travel into the U.S., and proscribes assistance and funding activities within the U.S. or by U.S. citizens.[63]

- Organizations, individuals or entities identified under Executive Order 13224. 219 as of November 2002. This Executive Order imposes penalties on the specific individuals and organizations named as terrorists and supporters of terrorism. It was designed primarily as a method of disrupting terrorist financing. Since it is an Executive Order, it may be updated to reflect changing conditions.

Other countries and the United Nations have similar, if varied, legal categories of "proscribed" organizations and individuals. Inclusion of a group on such lists of legally

---

[62] David Newman, ed., *Boundaries, Territory and Postmodernity* (Portland: Frank Cass Books, 1999), 17-20.
[63] Department of State, *Patterns of Global Terrorism 2001* (Washington, D.C., May 2002), 144.

designated groups is at the discretion of, and for the interests of, the state or organization compiling the list.

Conclusion

The intent of this chapter was to provide the reader with basic background information concerning the nature and history of terrorism. Terrorism is a particular tactic in political conflicts that is usable by individuals as well as nations. Due to its complexity it is difficult to define, but can be understood through varied combinations of description, observation, and terrorism historical review. Understanding the larger phenomenon of terror and terrorism is necessary before proceeding to the study of terrorists and their behaviors, motivations, and characteristics in Chapter 2.

Terrorism is foremost a political problem. Terminology and definition assists in determining the policy and processes to preclude, combat, or resolve acts of terrorism. To establish an appropriate national or international action plan to terrorism, action must consider aspects of terrorist activity that include political resolve and demonstration, criminal conduct, and possible links to paramilitary operations or low intensity conflict.[64]

To understand terrorism, the psychological impact of terror on a target audience must be viewed as a means to an end.

---

[64] Long, *The Anatomy of Terrorism,* 11 and 13.

Chapter 2
Terrorist Behaviors, Motivations, and Characteristics

Terrorists and terror groups constitute the enemy in the current Global War on Terrorism the United States finds itself engaged in today. However, despite decades of study, the nature of terrorists and their behaviors are hard to pin down. In addition to the difficulty in analyzing secretive, conspiratorial groups and individuals, the variety of motivations, ideologies, and behaviors involved gives the appearance of complete confusion. There seems to be no common characteristics or clearly defined traits that cut across the bewildering variety of terrorists and their organizations.

While all of this is true, there are benefits to studying terrorist motivations and behaviors, both at the individual and group level. Observations on human nature and group dynamics under the conditions of stress, excitement, and social isolation (to name just a few factors terrorists experience) can give us insight into the causes of particular behaviors. Also, understanding the various types of motivations for particular terrorists allows us to assess their stated aims against their actual intent. And despite the wide variety of individual terrorists, there are some practical observations about their general characteristics.

This chapter is organized into three sections. The first section is a discussion of terrorist behaviors and psychology at both individual and group level. The second examines the impact of group goals and motivations on their planning and operations. The third section consists of observations of general terrorist characteristics.

Section I: Terrorist Behavior

The common view of the terrorist is usually the unpredictable, viciously irrational stereotype colored by a lot of media images and sensationalism. However, as our examination of the nature and history of terrorism in Chapter 1 shows, terrorism is a rationally selected tactic, employed in the pursuit of political aims. Yet, to lend some truth to the cinema stereotype, the individuals or small organizations that employ terrorist tactics may in fact not always be concerned with particular causes or avowed ideology. Some may in fact be motivated purely by a need to be terrorists, in whatever cause suits them, or as a gun for hire serving a variety of causes.

This contradiction is summed up in the two most common approaches in analyzing terrorist group and individual behavior. They are:

- The psychologically compelled (sociopath or psychopath) model: This supposes that terrorists engage in terrorism because it fulfills a psychological need (not exclusively a need for violence) on their part. It treats avowed ideology and political causes, as after the fact justifications for behaviors the terrorist will commit anyway.

- The rational choice model: Terror is a tactic selected after rational consideration of the costs and benefits. The individual chooses participation in terrorist activities by a conscious decision (although they may not know what they are getting into). While it

acknowledges that individuals or groups may be predisposed to violence, this is not considered the determining factor in the choice to use or renounce terror.

Neither of these descriptions is universally applicable, with all groups or individuals conforming to one or the other. Aspects of both theories are observed in groups and individuals. As usual, the real world provides instances of both theories, and they should both be kept in mind when examining the actions of terrorists.[65]

Individual Terrorist Behaviors

> **"An opinion can be argued with; a conviction is best shot."**
>
> T.E. Lawrence (of Arabia)

No one profile exists for terrorists in terms of their backgrounds or personal characteristics. The differences in the origins of terrorists in terms of their society, culture, and environment preclude such a universal approach for foreign or domestic terrorists. The profiles developed for the typical West German Red Army Faction (RAF) member 15 years ago is irrelevant to predicting the nature of an Indonesian al Qaeda recruit. Trying to predicatively profile potential terrorists, even within the same culture, is a task beyond the scope of this work. But while we cannot predict the identity of future terrorists, there are some valid observations to be made of practicing terrorists. These consist of behaviors and attitudes to which such individuals conform.

Utopian Worldview

> **"…the time after victory, that is not our concern …We build the revolution, not the socialist model."**
>
> Gudrun Ensslin, co-leader, Red Army Faction

Terrorists typically have utopian goals, regardless of whether their aims are political, social, territorial, nationalistic, or religious. This utopianism expresses itself forcefully as an extreme degree of impatience with the rest of the world that validates the terrorists' extreme methods.[66] This philosophy may be best expressed as "Tear everything up; change now and fix later." The individual commonly perceives a crisis too urgent to be solved other than by the most extreme methods. Alternately, the perception is of a system too corrupt or ineffective to see or adopt the "solution" the terrorist expounds. This sense of desperate impatience with opposition is central to the terrorist worldview. This is true of both secular

---

[65] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 3 & 30.
[66] Ibid., 30.

and religiously motivated terrorists, although with slightly different perspectives as to how to impose their "solutions."

There is also a significant element of impracticability associated with this utopian mindset. Although their goals often involve the transformation of society, or a significant reordering of the status quo, individual terrorists, even the philosophical or intellectual leaders, are often vague or uncaring as to what the future order of things will look like or how they will be implemented. It seems that change, and the destructive method by which change is brought about, is much more important than the end result.

<u>Interaction with Others</u>

Terrorists interact within their groups with both other members and leadership. It is common for individuals forming or joining groups to adopt the "leader principle." This amounts to unquestioning submission to the group's authority figure. This is true of both hierarchical and networked organizations, and of large and small groups. It explains the prevalence of individual leaders of great charisma in many terrorist organizations.[67] With a predisposition to view leaders and authority figures within the group as near ideal examples, such leaders can demand tremendous sacrifices from subordinates. It also is a cause of the bitterness of internal dissension when a leader is at odds with the group, or factions arise in the organization.[68]

Another adaptation the individual makes is accepting an "in-group" (us against the world) mentality. This results in a presumption of automatic morality on the part of the other individual members of the group, and the purity of their cause and righteousness of their goals. It also involves the view of the wider world as aggressively attacking or persecuting the individual and his compatriots. Thus, violence is necessary for the "self-defense" of the group and carries moral justification. In some cases, the group comes to identify completely with their use of violence, and it becomes to them the defining characteristic of their existence on both the individual and collective level. Groups in this mind-set cannot renounce violence, since it would equal renouncing their own reason for being.[69]

<u>De-humanization of Non-members</u>

> **"Dear animal killing scum! Hope we sliced your finger wide open and that you now die from the rat poison we smeared on the razor blade."**
>
> Anonymous letter rigged with rat poison covered razor blades sent to 65 guide outfitters across British Columbia and Alberta from the "Justice Department" (radical animal rights group), January 1996

---

[67] Sabil Frances, "Uniqueness of LTTE's Suicide Bombers," *Institute of Peace and Conflict Studies*, Article no. 321 (4 February 2000): 1; available at http://www.ipcs.org; Internet; accessed 7 September 2002.

[68] Walter Lacquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (New York: Oxford University Press, 1999), 95.

[69] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 38.

There is a de-humanization of all "out-group" individuals. This de-humanization permits violence to be directed indiscriminately at any target outside the group. Assuming that all those outside of the group are either enemies or neutral, terrorists are justified in attacking anyone. And since anyone outside the group is a potential enemy, circumstances can change that permit any restraints that the terrorists might have observed to be broken in the name of expediency.

De-humanization also removes some of the onus of killing innocents. The identification of authority figures with animals makes murder a simple slaughter of inferior life. The continual picture held up to group members is that there are oppressors and oppressed; they are fighting inhuman opponents in the name of the oppressed.

This is the other aspect of de-humanization. By making "the oppressed" or "the people" an abstract concept, usually an ignorant mass, it permits the individual terrorist to claim to act on their behalf. The terrorist believes these acts further the interests of some "un-awakened" social or ethnic constituency that is too oppressed or misinformed to realize its interests. They see themselves as leading the struggle on behalf of the rest of whatever constituency they represent. This view on the part of terrorists is common to all shades of the political spectrum. It is variously identified as "the revolutionary vanguard" or "true patriots," but involves the terrorists acting for the good of either a silent or ignorant mass that would approve of their struggle if they were free to choose or if they understood.

Lifestyle Attractions

"There's something about a good bomb."

Bill Ayers, Former Weather Underground Leader
in his memoir "Fugitive Days"

Frequently, there is actual enjoyment of the lifestyle of a terrorist. While not particularly appealing for members of stable societies, there are emotional, physical and sometimes social rewards for being a terrorist. Emotional rewards include the feelings of notoriety, power, and belonging. In some societies, there may be a sense of satisfaction in rebellion; in others there may be a perceived increase in social status. For some, the intense sense of belonging generated by membership in an illegal group is emotionally satisfying.[70]

Physical rewards can include such things as money, authority, and adventure.[71] The lure of these things can subvert other motives. Several of the more notorious terrorists of the 1970s and 1980s, such as Abu Nidal,[72] became highly specialized mercenaries, discarding their convictions and working for a variety of causes and sponsors. Abu Nidal is a nom de guerre for Sabri al-Banna and an international terrorist group named after its founder "Abu Nidal" –

---

[70] Ibid.,34-35.
[71] Ibid., 271.
[72] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 187.

Abu Nidal Organization (ANO).[73]   Sabris al-Banna rose in notoriety in the Palestine Liberation Organization (PLO) but broke away from the PLO to form his own terror organization in the mid-1970s. The group's goals center on the destruction of the state of Israel, but the group has served as a mercenary terrorist force with connections to several radical regimes including Iraq, Syria, and Libya.[74] ANO activities link to terrorist attacks in 20 countries with killing about 300 people and injuring hundreds of additional people totaling estimates of about 900 victims.[75]

Lifestyle attractions also include a sense of elitism, and a feeling of freedom from societal mores. "Nothing in my life had ever been this exciting!" enthused Susan Stern, member of the Weather Underground, describing her involvement with the group.[76]

Behaviors Within Organizations

People within groups have different behaviors collectively than they do as individuals. This is as true of terrorists as it is of audiences at concerts or

> **Motivation for Destruction**
> Committing destructive acts for purely personal gratification is not confined to the alienation present in modern society. The Temple of Artemis at Epheseus was one of the ancient world's most famous buildings. It was renowned both for the richness of the furnishings and the splendor of the architecture. However, because of this fame, it became a target for an individual whose contribution to world history was self-aggrandizing destruction. Herostratus destroyed the Temple in 356 B.C.E., allegedly stating that the name of the man who had built it would be lost to history, but that the name of the man who destroyed such a wonder would live forever.

members of book clubs. Terrorist organizations have varying motives and reasons for existence, and how the group interprets these determines a great deal of the internal group dynamics. Again, no one profile or predictive tool works for various terror groups but some common features are set out below.

Groups are collectively more daring and ruthless than the individual members. No individual wishes to appear less committed than the others, and will not object to proposals within the group they would never entertain as an individual.[77] Leaders will not risk being seen as timid, for fear of losing their influence over the group. The end result can be actions not in keeping with individual behavior patterns as far as risk and lethality, but dictated by the pressure of group expectations and suppression of dissent and caution.

They stress secrecy and loyalty to the group. Disagreements are discouraged by the sense of the external threat represented by the outside world, and pressure to conform to the group view. Doubts about group goals and activities are suppressed, often by eliminating the doubters. No punishment is worse than excommunication from the group, and deserters are objects of universal loathing and hatred.[78] Even the slightest suspicion of disloyalty can result

---

[73] "Abu Nidal," *Encyclopedia of the Orient* [database on-line]; available from http://i-cias.com/e.o/abu_nidal.htm; Internet; accessed 24 February 2004.

[74] "Abu Nidal Organization," *Terrorism Questions and Answers* [database on-line]; available from http://cfrterrorism.org/groups/abunidal.html; Internet; accessed 24 February 2004.

[75] "Abu Nidal Organization (ANO)," *FAS Intelligence Resource Program* [database on-line]; available from http://www.fas.org/irp/world/para/ano.htm; Internet, accessed 24Febraury 2004.

[76] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 176.

[77] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 36.

[78] David C. Rapoport, ed*., Inside Terrorist Organizations* (New York: Columbia University Press, 1988), 157.

in torture and murder of the suspect. The ideological intensity that makes terrorists such formidable enemies often turns upon itself, and some groups have purged themselves so effectively that they almost ceased to exist.[79]

Frequently, the existence of the group becomes more important than the goal they originally embraced. If the group nears success, it will often "move the goalposts" so as to have a reason to continue to exist. In some cases, success will mean disbanding the organization, an option to be rejected by individuals or factions whose fundamental identity and personal worth is derived from being a terrorist. Factions that advocate keeping to the original objective will inspire bitter infighting and schism in the group. The resulting splinter groups or dissenting individual members are extremely volatile and run the risk of compromising the entire group.

In cases where the terrorists are not tied to a particular political or social goal, groups will even adopt a new cause if the original one is resolved. When first formed, many of the Euro-terror groups such as the Red Army Faction (Germany) and Communist Combatant Cells (Belgium) grew out of the 1960s student protest movement. The initial motivations for their actions were supposedly to protest U.S. involvement in Vietnam and support the North Vietnamese government. When American involvement in Vietnam came to an end, the radical left in Europe embraced Palestinian and pro-Arab causes rather than disband. Later, they conducted attacks against research facilities supporting the U.S. Strategic Defense Initiative, and to prevent deployment of the Pershing IRBM (Intermediate Range Ballistic Missile) in Germany. These examples of liberal, very left wing viewpoints illustrate that groups can align themselves with causes in keeping with their own goals and the way they visualize value. Understanding these linkages and associations are fundamental to "staying ahead" of emerging new threats.

Organizations that are experiencing difficulties may tend to increase their level of violence. This increase in violence can occur when frustration and low morale develops within the group due to lack of perceived progress or successful counter-terrorism measures that may limit freedom of action within the terrorist group. Members attempt to perform more effectively, but such organizational and cooperative impediments usually result in poor operational performance.   The organization hopes that a change to more spectacular tactics or larger casualty lists will overcome the group's internal problems.[80] An example of this occurred in Kashmir in 2003. After an increase in suicide attacks, Lieutenant General Hari Prasad, the chief of India's northern command in Kashmir stated that militants were launching attacks to lift the morale of their cadres, because continued Indian army operations were killing six to eight militants a day, thus weakening the groups.[81]

Another example of this phenomenon is the terrorist group, al Qaeda in the Arabian Peninsula. This regional arm of al Qaeda in Saudi Arabia is one of several associated sub-

---

[79] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 213.

[80] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 16.

[81] "Kashmir's Army Chief Fears Increased Suicide Attacks by Rebels," South Asia Monitor, 6 August 2003, 2; available from http://www.southasiamonitor.org/focus/2003/july/24rebels.html; Internet; accessed 20 April 2004.

groups in a larger global reach terrorist organization, al Qaeda. During a 13-month period, this al Qaeda sub-group sustained a number of arrests and killings of their members, including the group's leader being killed and replaced four times. In May and June 2004, the sub-group conducted a wave of hostage taking, beheadings, and gruesome murders. An interview by *Sawt Al-Jihad*, an al Qaeda identified journal, was conducted with the commander of the Al-Quds Brigade, a subordinate unit of the group that took responsibility for the May 29, 2004 Oasis Compound attack at al-Khobar, Saudi Arabia where 22 people were killed. During this interview, the terrorist commander claimed they had either beheaded or cut the throats of more than 12 of the victims.[82] Al Qaeda in the Arabian Peninsula was also responsible for a number of other murders, including the killing of Robert Jacobs, an American employee of Vinnell Corporation, and the beheading of Paul Johnson, an American employee of Lockheed-Martin. In both of these, the terrorist group released gruesome videos of the murders. This increase in violence may very well be the result of the successful attacks against the group by Saudi security forces.

Section II: Impact of Terrorist Goals & Motivations on Planning

Practical strategies against terrorists require consideration of the terrorist's point of view in his targeting and operations. Understanding the opponents' preferences and capabilities allows better defense and promotes an active approach to the threat. Total interdiction of all possible targets is impossible, since the defender cannot protect everything. While consistent prediction is unlikely, accurate determination of what risks are acceptable must consider the terrorists' values, particularly their estimate of the target's value, and the costs of the operation necessary to successfully hit it.

The proliferation of terrorism expertise, and the breakdown in restraint and observance of international norms allow many more groups and individuals to use terror as a viable tool[83] in order to achieve their goals. With more potential terror users, the U.S. will often be a terrorist target for several reasons.

There has been an increase in transnational radicalism as compared to recent historical conflicts. As the most prominent secular democracy and largest single economic, military, and political power in the world, the U.S. becomes an easy and appealing target for extremists. Additionally, since the United States declared the Global War on Terrorism, the U.S. has become the principal opponent of extremists throughout the world. Much of the current thinking and literature on terrorism developed when terrorism was closely tied to revolutionary movements and separatist movements concerned with influencing events in relation to one nation. Newer causes and ideologies, such as religion, economic concerns, or environmental issues are international, transnational, or even global in scope.

Further, the perception that the U.S. is the single most powerful nation in the world invites targeting by terror groups regardless of ideology to demonstrate their power and status. In the worldview of many terrorist groups, the perceived power and influence of the U.S.

---

[82] *Al-Qaeda in the Arabian Peninsula: Shooting, Hostage Taking, Kidnapping Wave – May/June 2004* (Alexandria: Tempest Publishing, LLC, 2004), 46-60.
[83] Martha Crenshaw, "The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice," in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed., ed. Walter Reich (Washington: Woodrow Wilson Center Press, 1998), 14.

encourages targeting to force the U.S. to extract concessions from third parties (prisoner release, policy changes, etc.). Although some people may question why a comparatively small terrorist group believes it can successfully confront the United States, part of the answer lies in the Afghanistan jihad fighters and their success against the Soviet Union. Many of these Islamic fighters were persuaded that they alone had defeated the Soviet Union in Afghanistan (even though the U.S. provided substantial support) and that they could do the same to the United States.[84]

Another reason to expect greater use of terrorism against the U.S. is that possible competitors may feel that they cannot openly challenge or defeat the U.S. with any other technique. Nations have employed state sponsored terrorism to produce results that could not have otherwise been achieved against U.S. opposition. The current supremacy of American military power leaves adversaries with few options to challenge U.S. interests. Adding non-state groups of formidable capability and few restraints to the roster of potential adversaries of the U.S. increases the likely use of terror against our forces.

Many potential adversaries view the U.S. as particularly vulnerable to the psychological impact and uncertainties generated by terror tactics in support of other activities.[85] Terrorism and terror tactics have already been used against U.S. forces in support of conventional and insurgent warfare, as well as against U.S. forces during stability and peace support operations in attempts to influence policy. Lessons drawn from previous uses of terror against the U.S. have led to some commonly held perceptions about the effectiveness and impact of terrorism versus the U.S. Some of these perceptions may or may not be valid, but are still widely held. Consequently, terrorist groups are likely to try to capitalize on what they may perceive as vulnerabilities. They include the beliefs that:

The U.S. is extremely casualty averse. Any loss of life takes on significance out of proportion to the circumstances.

> **"We have seen in the last decade the decline of the American government and the weakness of the American soldier who is ready to wage Cold Wars and unprepared to fight long wars. This was proven in Beirut when the Marines fled after two explosions. It also proves they can run in less than 24 hours, and this was also repeated in Somalia."**
>
> Usama bin Laden interview by ABC News' John Miller, May 1998

The U.S. Government policies and policy makers are overly influenced by public opinion, which in turn is particularly susceptible to the adverse psychological impact of terrorism.

---

[84] Gilles Kepel, *Jihad: The Trail of Political Islam* (Cambridge: The Belknap Press of Harvard University Press): 10,17.

[85] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare,* trans. Department of State, American Embassy Beijing Staff Translators (Washington, D.C., 1999).

> **"We are an instrument for the hostages… We force the Administration to put their lives above policy."**
>
> Lesley Stahl, CBS White House correspondent
> during the TWA flight 847 hostage crisis, 1985

The U.S. economic performance is perception driven, and therefore equally vulnerable to the adverse psychological impact of terrorism.

> **"Whoever has stolen our wealth, then we have the right to destroy their economy."**
>
> Usama bin Laden's "Letter to America"
> Sunday November 24, 2002

The U.S. cannot sustain long-term efforts, or exhibit public sacrifice in pursuit of difficult national goals.

> **"Those youths are different from your soldiers. Your problem will be how to convince your troops to fight, while our problem will be how to restrain our youths to wait for their turn in fighting and in operations."**
>
> Usama bin Laden, "Declaration Of War Against The Americans
> Occupying The Land Of The Two Holy Places" August 26, 1996

Finally, the growing polarization of some domestic political issues means that the U.S. is also likely to see increased terror attacks on its own soil by a variety of "home-grown" groups. These groups may target U.S. forces either as symbols, sources of weapons and equipment, or at the behest of other terrorist groups in exchange for money or support elsewhere.

Terrorist Asset Cost versus Target Value

Despite popular perception, there are not an unlimited number of terrorists. They require recruitment, preparation, and integration into the operational structure of the group. Recruits also require extensive vetting to ensure that they are not infiltrators from enemy security forces. For this reason, they are valuable assets, which a group's leadership will not employ without serious consideration of the relationship between the cost of using (and possibly

losing) the asset, and the potential benefits to the group. While some groups may have a greater supply of personnel assets than others, no group can expend them injudiciously.[86] Therefore terrorist operational planning focuses on economies of personnel, and balances the likelihood of losses against the value of a target and the probability of success. This is why suicide bombings are on the increase – large payoff for low cost.

In any terrorist operation, extensive pre-operational surveillance and reconnaissance, exhaustive planning, and sufficient resources will be committed to the operation.[87] The potential risk of exposure of these resources, and the demands on their time, must be factored into the equation when deciding to commit to an attack.

Operational Intent of Terrorism

It is vital to remember that terrorism is a psychological act. It is communication through the medium of violence directed at others. This requirement to reach a target audience with the intended psychological impact results in terrorist planning exhibiting many differences from military planning or "rational" game strategies. Terrorist strategies will be aimed at publicly causing damage to symbols or inspiring fear. Timing, location, and method of attacks are designed to accommodate media dissemination and ensure "newsworthiness" to maximize impact.

A terrorist operation will often have the ultimate goal of manipulating popular perceptions, and it will achieve this by controlling or dictating media coverage. This control need not be overt, as terrorists analyze and exploit the dynamics of major media outlets and the pressure of the "news cycle."[88] A terrorist attack that appears to follow this concept was the bombing of commuter trains in Madrid, Spain in March 2004. There has been much speculation as to the true objective behind these bombings.   One view is that Islamic terrorists who specifically planned to influence the political process in Spain conducted the attacks. They believed that the large percentage of the Spanish population opposed the war in Iraq and would feel that the current government was responsible for the bombings, and would therefore vote for the opposition.   The attacks occurred during morning rush hour just three days prior to national elections. The timing facilitated maximum casualties on the trains (killing 191 people and injuring more than 1800), plus immediate news coverage throughout the world of the carnage resulting from this terrorist attack. Although it cannot definitively be linked to the bombings, an anti-war Socialist prime minister was elected who quickly withdrew Spain's military forces from Iraq.

In considering possible terrorist targets, recognize that a massively destructive attack launched against a target that cannot or will not attract sufficient media coverage to impact the target audience is not a viable target for terrorists. A small attack against a "media accessible" target is better than a larger one of less publicity. However, the spread of the global media makes many locations attractive targets that would not have been remotely considered thirty or forty years ago. The 1998 bombings of the American embassies in

---

[86] Ehud Sprinzak, "Rational Fanatics," *Foreign Policy,* no. 120 (September/October 2000): 66-73.

[87] Rohan Gunaratna, "Suicide Terrorism: a Global Threat," *Jane's Intelligence Review* (20 October 2000): 1-7; available from http://www.janes.com/security/international_security/news/usscole/jir001020_1_n.shtml; Internet; accessed 7 September 2002.

[88] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 136-142.

Kenya and Tanzania illustrate how these two relatively unimportant posts created a global sensation because of the media coverage. Forty years ago it would have taken days for the international news media to get still photographs and some text from these locations, making them much less attractive targets. However, with today's modern technology, media reporters were able to provide immediate broadcast coverage of the bombings. Since the Islamist factions that conducted the attacks used religious justifications for their actions, the worldwide coverage of these attacks made it possible for these terrorists to pose as champions of the cause, even in the absence of any effective work at the grassroots level of society.[89] The September 11, 2001 bombing of the World Trade Center in New York City was observed by millions of people worldwide on live television as the successive attacks occurred, and sensational mass destruction followed.

Ideology and Motivation Influences on Operations

Ideology and motivation will influence the objectives of terrorist operations, especially regarding the casualty rate. Groups with secular ideologies and non-religious goals will often attempt highly selective and discriminate acts of violence to achieve a specific political aim. This often requires them to keep casualties at the minimum amount necessary to attain the objective. This is both to avoid a backlash that might severely damage the organization, and also maintain the appearance of a rational group that has legitimate grievances. By limiting their attacks they reduce the risk of undermining external political and economic support. A good illustration of a group that discriminates on target selection is the Revolutionary Organization 17 November. This is a radical leftist organization established in 1975 in Greece that is anti-Greek establishment, anti-United States, anti-Turkey, and anti-NATO. Its operations have included assassinations of senior U.S. officials, Greek public figures, European Union facilities, and foreign firms investing in Greece. Although a violent organization, reports are the group did not kill a bystander until 1992. In total, 17 November is believed to have been responsible for over 100 attacks, but just 23 fatalities between 1975 and 2000. [90] Groups that comprise a "wing" of an insurgency, or are affiliated with above-ground, sometimes legitimate, political organizations often operate under these constraints. The tensions caused by balancing these considerations are often a prime factor in the development of splinter groups and internal factions within these organizations.

In contrast, religiously oriented and millenarian groups typically attempt to inflict as many casualties as possible. An apocalyptic frame of reference may deem loss of life as irrelevant and encourage mass casualty producing incidents. Losses among their co-religionists are of little account, because such casualties will reap the benefits of the afterlife. Likewise, non-believers, whether they are the intended target or collateral damage, deserve death, and killing them may be considered a moral duty. The Kenyan bombing against the U.S. Embassy in 1998 inflicted casualties on the local inhabitants in proportion to U.S. personnel of over twenty to one killed, and an even greater disparity in the proportion of wounded (over 5000 Kenyans were wounded by the blast; 95% of total casualties were non-American).[91]

---

[89] Gilles Kepel, *Jihad: The Trail of Political Islam* (Cambridge: The Belknap Press of Harvard University Press): 320.

[90] "Revolutionary Organization 17 November (17N)," CDI Terrorism Project, 5 August 2002; available from http://www.cdi.org/terrorism/17N-pr.cfm; Internet; accessed 24 September 2004.

[91] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 51.

Fear of backlash rarely concerns these groups, as one of their goals may be to provoke overreaction by their enemies and potentially widen the conflict. In the case of the Embassy bombing in Kenya, the suicide bomber failed in his attempt to penetrate the Embassy's outer perimeter, thanks to the refusal of local guards to open the gates. This resulted in the large casualty rate amongst local Kenyans. With numerous dead and maimed Kenyans, the terrorists issued a statement attempting to qualify a rationale for the deaths and to mollify critics.

The type of target selected will often reflect motivations and ideologies. For groups professing secular political or social motivations, their targets are highly symbolic of authority; government offices, banks, national airlines, and multinational corporations with direct relation to the established order. Likewise, they conduct attacks on representative individuals whom they associate with economic exploitation, social injustice, or political repression. While religious groups also use much of this symbolism, there is a trend to connect it to greater physical devastation. There also is a tendency to add religiously affiliated individuals, such as missionaries, and religious activities, such as worship services, to the targeting equation.

Another common form of symbolism utilized in terrorist targeting is striking on particular anniversaries or commemorative dates. Nationalist groups may strike to commemorate battles won or lost during a conventional struggle, whereas religious groups may strike to mark particularly appropriate observances. Many groups will attempt to commemorate anniversaries of successful operations, or the executions or deaths of notable individuals related to their particular conflict. Likewise, striking on days of particular significance to the enemy can also provide the required impact. For instance, Timothy McVeigh conducted the bombing of the Murrah Federal Building on April 19th, the anniversary of the end of the Branch Davidian siege near Waco, Texas. Since there are more events than operations, assessment of the likelihood of an attack on a commemorative date is only useful when analyzed against the operational pattern of a particular group or specific members of a group's leadership cadre.

Section III: Terrorist Characteristics

There is no single personality profile of a terrorist, and no predictive test that can reliably identify one. However, there are some general characteristics that are fairly common among terrorists. There are also some common stereotypes and misperceptions regarding the terrorists that are widely held, but inaccurate.

Status

Contrary to the oft-repeated charge that terrorism is a product of poverty and despair, terrorists are most commonly from middle class backgrounds, with some actually coming from extreme wealth and privilege. While guerilla fighters and gang members often come from poor and disadvantaged backgrounds, and may adopt terrorism as a tactic, terrorist groups that specifically organize as such generally come from middle and upper social and economic strata. The leadership may use less educated and socially dispossessed people to conduct acts of terrorism. Even in terrorist groups that espouse the virtues of "the people" or "the proletariat," leadership consists primarily of those of middle class backgrounds. However, this characteristic must be considered in context with the society the terrorist originates from.

"Middle class" or "privilege" are relative terms and will, for example, mean completely different levels of income between West Africa and Western Europe.

Education and Intellect

Some leaders of larger terrorist organizations may have minimal education, but this characteristic is not the norm. Left wing terrorists, international terrorists, and the leadership echelon of right wing groups are usually of average or better intelligence, and have been exposed to advanced education. (Usama bin laden and Yasir Arafat are civil engineers and Ayman Zawahiri is a physician.) These terrorists generally have had exposure to higher learning, although they are usually not highly intellectual, and are frequently dropouts or possess poor academic records. Again, this is subject to the norms of the society they originate from. In societies where religious fundamentalism is prevalent, the higher education may have been advanced religious training.[92]

Domestic and right wing terrorists tend to come from lower educational and social levels, although they are not uneducated. It was right wing domestic groups in the U.S. that first explored the communication and organizational potential of the Internet. They will typically have received a high school level education, and be very well indoctrinated in the ideological arguments they support.

Age

Terrorists tend to be young. Leadership, support, and training cadres can range into the 40-50 year old age groups, but most operational members of terrorist organizations are in the 20-35 year old age group.[93] The amount of practical experience and training that contributes to making an effective operative is not usually present in individuals younger than the early 20s. Individuals in their teens have been employed as soldiers in guerilla groups, but terrorist organizations do not tend to accept extremely young members, although they will use them as non-operational supporters. Groups that utilize suicide operations will employ very young individuals as suicide assets, but these youths are not actually members of the organization, but simply exploited or coerced into an operational role.[94] An exception is the Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka. They have recruited children to offset a manpower shortage due to casualties. Assessments by the Sri Lankan Directorate of Military Intelligence indicate a large percentage of fighters are below 18 years of age.[95]

Gender

Terrorists are not exclusively male, even in groups that are rigorously Islamic. Women's roles in these groups will often be constrained to support or intelligence work, but some fundamentalist Islamic groups use women in operational roles. In groups where religious

---

[92] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 208.

[93] Walter Lacquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (New York: Oxford University Press, 1999), 38.

[94] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 270.

[95] "Liberation Tigers of Tamil Eelam (LTTE)," South Asia Terrorism Portal, n.d., 2; available from http://www.satp.org/satporgtp/countries/shrilanka/terroristoutfits/Ltte.htm; Internet; accessed 7 July 2004.

constraints do not affect women's roles, female membership may be above fifty percent, with women fully integrated into operations. Female leadership of terrorist groups is not uncommon, and female terrorists lack for nothing in terms of violence and ruthlessness. For example, one-third of the LTTE cadre is made up of women and it is reported that nearly 4,000 have been killed since they began taking part in combat in 1985, over 100 of those killed belonging to the dreaded Black Tiger suicide squad.[96]

Again, there is an exception to this general observation in some right wing groups, particularly those with neo-Nazi and Christian Identity oriented ideologies. Female participation and leadership is much less common in these groups.

Appearance

Terrorists are often unremarkable individually. Racial diversity in organizations such as al Qaeda signal that attempts to racially profile likely terrorist group members is not an effective indicator. They usually do not appear out of the ordinary, and are capable of normal social behavior and appearance. Over the long term, elements of fanatical behavior or ruthlessness may become evident, but they are typically not immediately obvious to casual observation. An excellent example of this is the group 17 November in Greece. When the police captured 14 suspected members in 2002, the most striking characteristic was their ordinary nature. Among the group were a schoolteacher, a shopkeeper, a telephone operator, and other members that appeared to be members of mainstream society.[97] Although members of sleeper cells or other covert operators may marry as part of their persona, most terrorists do not marry, even though there have been cases of married couples within terrorist organizations.

Conclusion

This chapter provided a discussion of some aspects of terrorist behavior and group dynamics. This information will allow the reader to place these behaviors in context with the descriptions of terrorist organizations in Chapter 3.

---

[96] Ibid., 2.
[97] "Revolutionary Organization 17 November (17N)," CDI Terrorism Project, 5 August 2002; available from http://www.cdi.org/terrorism/17N-pr.cfm; Internet; accessed 24 September 2004.

Chapter 3
Terrorist Group Organization

This chapter examines terrorist group organization. Joint Publication 3-07.2 *Joint Tactics, Techniques, and Procedures (JTTP) for Antiterrorism* (Revised First Draft) states that, "The terrorist organization's structure, membership, resources, and security determine its capabilities and reach." A general knowledge of the prevalent models of terrorist organizations leads to a better understanding of their overall capabilities. Knowledge of the different labels and systems of classification that have been applied to groups and individuals aid us in discarding useless or irrelevant terms, and in correctly using the commonly accepted descriptions of terrorism.

Traditionally, a popular image of a terrorist group operating according to a specific political agenda and motivated by ideology or the desire for ethnic or national liberation dominated our understanding of terrorism. While still true of some terrorist organizations, this image is no longer universally valid. Also, a generational change in leadership of established groups is in many cases ushering in a more destructive and relentless type of organization.

When examining the overall structure of terrorist groups, there are two general categories of organization: networked and hierarchical. A terrorist group may employ either type or a combination of the two models. Newer groups tend towards organizing or adapting to the possibilities inherent in the network model. Ideology can have an effect on internal organization, with strict Leninist or Maoist groups tending towards centralized control and hierarchical structure. Within the larger structure, though, virtually all groups use variants of cellular organizations at the tactical level to enhance security and to organize for operations.

Terrorist groups that are associated with a political activity or organization will often require a more hierarchical structure, in order to coordinate terrorist violence with political action. It also can be necessary for a politically affiliated group to observe "cease-fires" or avoid particular targets in support of political objectives. This can be difficult to enforce in networked organizations.

Terrorist groups can be at various stages of development in terms of capabilities and sophistication. Newer groups with fewer resources will usually be less capable, and operate in permissive areas or under the tutelage of more proficient organizations to develop proficiency. Change in terrorist leadership, whether through generational transition or as a response to enhanced security operations, may signal significant adjustments to organizational priorities and means of conducting terrorism. Also, groups professing or associated with ethnic or nationalist agendas and limiting their operations to one country or a localized region tend to require fewer capabilities. Larger groups can coalesce from smaller organizations, or smaller groups can splinter off from larger ones.

Section I: Terrorist Group Structure

> **"There's nothing wrong with being a terrorist, as long as you win."**
> Paul Watson, Sea Shepard Conservation Society

Levels of Commitment

There are typically different levels of commitment within an organization: passive supporters, active supporters, cadre, and leadership. Figure 3-1 shows how each successive level of commitment has fewer members. This pyramid diagram is not intended as an organizational picture, but to show the relative number of people in each category. This image of overall density holds true for networks as well as hierarchies. Passive supporters may intermingle with active supporters and be unaware of what their actual relationship is to the organization.

- Leaders provide direction and policy; approve goals and objectives; and provide overarching guidance for operations. Usually leaders rise from within the ranks of any given organization, or create their own organization from scratch.

- Cadres are the active members of the terrorist organization. This echelon plans and conducts not only operations, but also manages areas of intelligence, finance, logistics, information operations, and communications. These activities all occur in the active membership. Mid-level cadres tend to be trainers and technicians such as bomb makers, financiers, and surveillance experts. Low-level cadres are the bombers and similar direct action terrorists in an attack.

- Active Supporters are active in the political, fund-raising, and information activities of the group. Acting as an ally or tacit partner, they may also conduct initial intelligence and surveillance activities, and provide safehaven houses, financial contributions, medical assistance, and transit assistance for active members of the organization. They are usually fully aware of their relationship to the terrorist group but do not commit violent acts.

- Passive Supporters are typically individuals or groups that are sympathetic to the announced goals and intentions of the terrorist organization, but are not committed enough to take action. They may not be aware of their precise relation to the terrorist group, and interface with a front that hides the overt connection to the terrorist group. Sometimes fear of reprisal from terrorists is a compelling factor in passive support. Sympathizers can be useful for political activities, fund raising, and unwitting or coerced assistance in intelligence gathering or other non-violent activities.
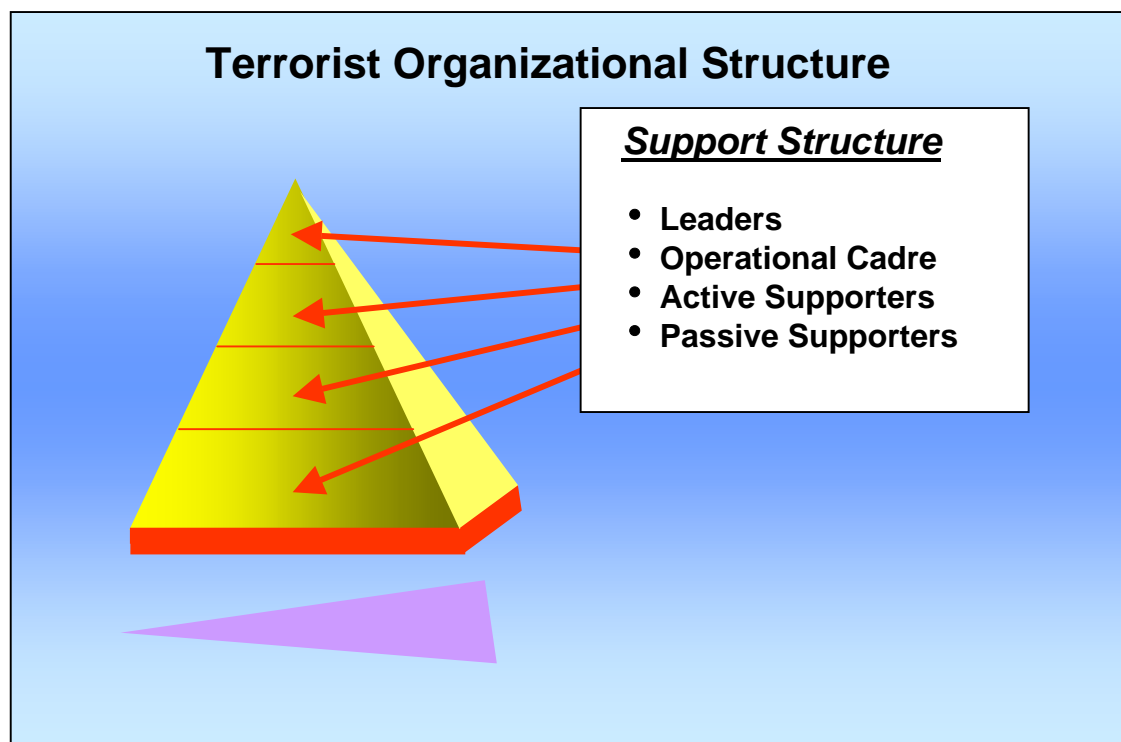
Figure 3-1. Typical Levels of Support

Terrorist groups will recruit from populations that are sympathetic to their goals. Often legitimate organizations can serve as recruiting grounds for terrorists. Militant Islamic recruiting, for example, is often associated with the proliferation of the radical Wahhabi sect. This recruiting is conducted on a worldwide basis via Wahhabist schools financed from both governmental and non-governmental donations and grants.[98] Some recruiting may be conducted for particular skills and qualifications, and not be tied to ideological characteristics. Of particular concern are attempts of terrorist organizations to recruit current or former members of the U.S. armed forces, both as trained operatives, and as agents in place.

Recruitment can gain operatives from many diverse social backgrounds. At times, the approach to radical behavior or direct actions with terrorism can develop over the course of years or decades. One example is John Walker Lindh, the U.S. citizen captured by U.S. military forces in the war in Afghanistan. His notoriety jumped into international attention, as did the situation of individuals from several counties that were apprehended in combat actions of Afghanistan. Lindh's change from an unassuming middle-class adolescent in the Western United States to a member of a paramilitary training camp in Pakistan and subsequent support for Taliban forces in Afghanistan spotlights that general profiling should be tempered with specific instances and a wide lens. In the case of Jose Padilla, his simple and voluntary efforts to detonate a bomb in the U.S. may illustrate al Qaeda techniques to support, finance, and use less than sophisticated means to conduct terrorist acts.

---

[98] Victor N. Corpus, "The Invisible Army" (Briefing presented at Fort Leavenworth, KS, 5 November 2002), TRADOC ADCSINT-Threats Files, Fort Leavenworth, KS.

Some groups will also use coercion and leverage to gain limited or one-time cooperation from useful individuals. This cooperation can range anywhere from gaining information to conducting a suicide bombing operation.[99] Blackmail and intimidation are the most common forms of coercion. Threats to family members are also employed. Coercion is often directed at personnel in government security and intelligence organizations.

Tactical-level Cellular Organization

The smallest elements at the tactical level of terrorist organizations are the cells that serve as building blocks for the terrorist organization. One of the primary reasons for a cellular or compartmentalized structure is security. The compromise or loss of one cell should not compromise the identity, location, or actions of other cells. A cellular organizational structure makes it difficult for an adversary to penetrate the entire organization. Personnel within one cell are often unaware of the existence of other cells and, therefore, cannot divulge sensitive information to infiltrators or captors. The home page of the Earth Liberation Front is an excellent example of this cellular organization. It states, "Modeled after the Animal Liberation Front, the E.L.F. is structured in such a way as to maximize effectiveness. By operating in cells (small groups that consist of one to several people), the security of group members is maintained. Each cell is anonymous not only to the public but also to one another. This decentralized structure helps keep activists out of jail and free to continue conducting actions."

Terrorists may organize cells based on family or employment relationships, on a geographic basis, or by specific functions such as direct action and intelligence. The terrorist group may also form multifunctional cells. The terrorist group uses the cells to control its members. Cell members remain in close contact with each other in order to provide emotional support and to prevent desertion or breach of security procedures. The cell leader is normally the only person who communicates and coordinates with higher levels and other cells.

A terrorist group may form only one cell or may form many cells that operate locally, transnationally, or internationally. The number of cells and their composition depend on the size of the terrorist group. A terrorist group operating within one country frequently has fewer cells and specialized teams than does an international terrorist group that may operate in several countries.

Group Organizational Structure

As stated earlier, there are two basic models used when examining the overall organizational structure of a terrorist group. These are the hierarchical and the networked models. A terrorist group may employ either type or a combination of the two models.

---

[99] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 270-271.
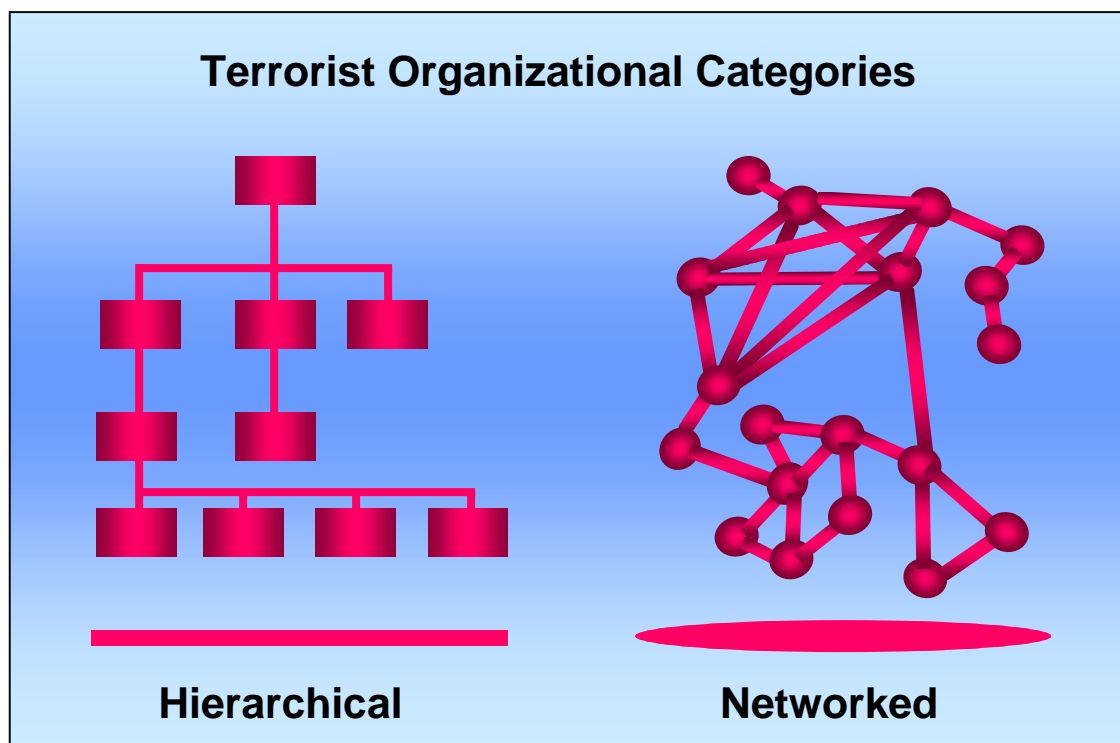
Figure 3-2. Typical Categories of Terrorist Organization

Hierarchical Structure

Hierarchical structure organizations are those that have a well-defined vertical chain of command linkage and responsibility. Data and intelligence flows up and down organizational channels that correspond to these vertical chains, but may not move horizontally through the organization. This is more traditional, and is common of groups that are well established with a command and support structure.

Hierarchical organizations feature greater specialization of functions in their subordinate cells (support, operations, intelligence). Usually, only the cell leader has knowledge of other cells or contacts, and only senior leadership has visibility of the organization at large. In the past, terrorism was practiced in this manner by identifiable organizations with a command and control structure influenced by revolutionary theory or ideology. Radical leftist organizations such as the Japanese Red Army, the Red Army Faction in Germany, the Red Brigades in Italy, as well as ethno-nationalist terrorist movements such as the Palestine Liberation Organization, the Irish Republican Army and the Basque separatist ETA group, conformed to this stereotype of the "traditional" terrorist group. These organizations had a clearly defined set of political, social or economic objectives, and tailored aspects of their organizations (such as a "Political" wing or "social welfare" group) to facilitate their success. The necessity to coordinate actions between various "fronts," some of which were political

and allegedly non-violent, and the use of violence by terrorists and some insurgents, favored a strong and hierarchical authority structure.

Networked Structure

Terrorists are now increasingly part of far more amorphous, indistinct and broader networks than previously experienced. Groups based on religious or single-issue motives lack a specific political or nationalistic agenda; they therefore have less need for a hierarchical structure to coordinate the achievement of their goals. Instead, they can depend and even thrive on loose affiliation with like-minded groups or individuals from a variety of locations. General goals and targets are announced, and individuals or cells are expected to use flexibility and initiative to conduct the necessary action.

Basic Concepts.

Networks consist of nodes. A node may be an individual, a cell, another networked organization, or a hierarchical organization. They may also consist of parts of other organizations, even governments, which are acting in ways that can be exploited to achieve the network's organizational goals.

The effectiveness of a networked organization is dependent on several things. The network achieves long-term organizational effectiveness when the nodes share a unifying ideology, common goals or mutual interests.[100] When there is failure to accept the overall goals of the organization, pieces of the network will drop out. This is less catastrophic than a splintering within a hierarchical group, but too many losses will render the organization ineffective.

Another difficulty for network organizations not sharing a unifying ideology is that nodes can pursue objectives or take actions that do not meet the goals of the organization, or are actually counterproductive. In this instance, the independence of nodes fails to develop synergy between their activities or contribute to common objectives.

Networks distribute the responsibility for operations, and provide redundancies for key functions. The various cells need not contact or coordinate with other cells except for those essential to a particular operation or function. The avoidance of unnecessary coordination or command approval for action provides deniability to the leadership and enhances operational security.

Networks are not necessarily dependent on the latest information technology for their effect. The organizational structure and the flow of information inside the organization are the defining aspects of networks. While information technology can make networks more effective, low-tech means such as couriers and landline telephones can enable networks to operate effectively in certain circumstances.

---

[100] John Arquilla and David Ronfeldt, ed., *Networks and Netwars* (Santa Monica: RAND, 2001), 9.

Basic Types.

There are various types of networked structure, depending on the ways in which elements are linked to other elements of the structure. There are three basic types: chain, hub, and all-channel. A terrorist group may also employ a hybrid structure that combines elements of more than one network type.

- Chain Networks

  Each node links to the node next in sequence. Communication between the nodes is by passing information along the line. This organization is most common among networks that smuggle goods and people or launder money.
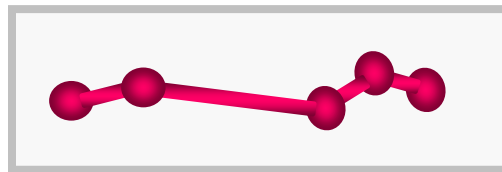

Figure 3-3. Chain Network

- Hub or Star and Wheel

  Nodes communicate with one central node. The central node need not be the leader or decision maker for the network. A variation of the hub is a wheel design where the outer nodes communicate with one or two other outer nodes in addition to the hub. A wheel configuration is a common feature of a financial or economic network.
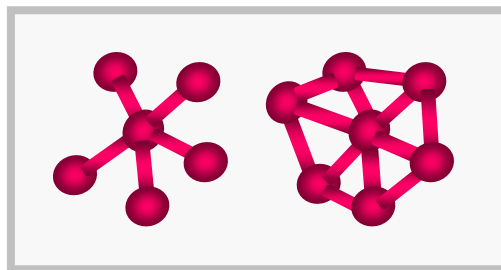

Figure 3-4. Hub - Wheel Network

- All-Channel

  All nodes are connected to each other. The network is organizationally "flat," meaning there is no hierarchical command structure above it. Command and control is distributed within the network. This is communication intensive and can be a security problem if the linkages can be identified or reconstructed. However, the lack of an identifiable "head" confounds targeting and disruption efforts normally effective against hierarchies.
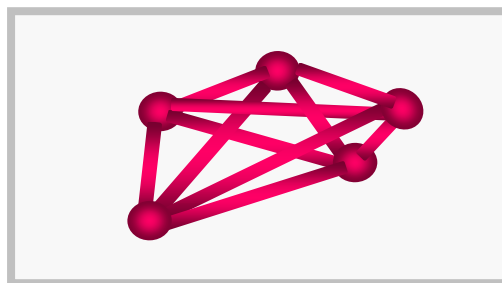

Figure 3-5. All Channel Network

Despite their differences, the three basic types will most likely be encountered together in hybrid organizations, where the particular organizational capability of a hybrid network type is most appropriate. Thus, a transnational terrorist organization might use chain networks for its money-laundering activities, tied to a wheel network handling financial matters, tied in turn to an all-channel leadership network to direct the use of the funds into the operational activities of a hub network conducting pre-targeting surveillance and reconnaissance. Organizational structure that may appear very complex during initial assessments of terrorist groups may be more understandable when viewed in the context of chain, hub variants, or all-channel networks.

Section II: Categories of Terrorist Organizations

There are many different categories of terrorism and terrorist groups that are currently in use. These categories serve to differentiate terrorist organizations according to specific criteria, which are usually related to the field or specialty of whoever is selecting the categories. Also, some categories are simply labels appended arbitrarily or redundantly, often by the media. For example, every terrorist organization is by definition "radical," as terror tactics are not the norm for the mainstream of any group. While this guide does not employ these categories in describing the operational aspect of terrorist groups, some categories do provide pertinent descriptive information. Doctrinal terrorism can be described as based on a universalistic political ideology or religious dogma. This is in contrast to nationalist-ethnic terrorism that centers on national or ethnic identity.[101] This section addresses many of the more common classifications, and provides explanation of terms and their relationship.

---

[101] Long, *The Anatomy of Terrorism,* 65.

Government Affiliation Categories

Categorizing terrorist groups by their affiliation with governments provides indications of their means for intelligence, operations, and access to types of weapons. U.S. joint doctrine identifies three affiliations: non-state supported, state-supported, and state-directed terrorist groups.[102]

- Non-state supported. These are terrorist groups that operate autonomously, receiving no significant support from any government.

- State-supported. These are groups that generally operate independently but receive support from one or more governments.

- State-directed. These groups operate as an agent of a government and receive substantial intelligence, logistic, and operational support from the sponsoring government.

Motivation Categories

Motivation categories describe terrorist groups in terms of their ultimate goals or objectives. While political or religious ideologies will determine the "how" of the conflict, and the sort of society that will arise from a successful conclusion, motivation is the "what"; what the end state or measure of success is. Some of the common motivation categories are:

- Separatist. Separatist groups are those with the goal of separation from existing entities through independence, political autonomy, or religious freedom or domination. The ideologies separatists subscribe to include social justice or equity, anti-imperialism, as well as the resistance to conquest or occupation by a foreign power.

- Ethnocentric. Groups of this persuasion see race as the defining characteristic of a society, and therefore a basis of cohesion. There is usually the attitude that a particular group is superior because of its inherent racial characteristics.

- Nationalistic. The loyalty and devotion to a nation, and the national consciousness derived from placing one nation's culture and interests above those of other nations or groups is the motivating factor behind these groups. This can find expression in the creation of a new nation, or in splitting away part of an existing state to join with another that shares the perceived "national" identity.

- Revolutionary: These groups are dedicated to the overthrow of an established order and replacing it with a new political or social structure. Although often associated with communist political ideologies, this is not always the case, and other political movements can advocate revolutionary methods to achieve their goals.

---

[102] Joint Pub 3-07.2. *Joint Tactics, Techniques, and Procedures for Antiterrroism*, 17 March 1998, II-6. [Revision First Draft dated 9 April 2004 exists at time of publication]

> **"From fanaticism to barbarism is only one step."**
> Denis Diderot

Ideological Categories

Ideological categories describe the political, religious, or social orientation of the group. While some groups will be seriously committed to their avowed ideologies, for others, ideology is poorly understood, and primarily a rationale used to provide justification for their actions to outsiders or sympathizers. It is a common misperception to believe that ideological considerations will prevent terrorists from accepting assistance or coordinating activities with terrorists or states on the opposite side of the religious or political spectrum. Quite often terrorists with differing ideologies have more in common with each other than with the mainstream society they oppose.[103] Common ideological categories include:

<u>Political</u>

Political ideologies are concerned with the structure and organization of the forms of government and communities. While observers outside terrorist organizations may stress differences in political ideology, the activities of groups that are diametrically opposed on the political spectrum are similar to each other in practice.

- Right wing: These groups are associated with the reactionary or conservative side of the political spectrum, and often, but not exclusively, are associated with fascism or neo-Nazism. Despite this, right-wing extremists can be every bit as revolutionary in intent as other groups, the difference being that their intent is to replace existing forms of government with a particular brand of authoritarian rule.

- Left wing: These groups are usually associated with revolutionary socialism or variants of communism (i.e. Maoist, Marxist-Leninist, etc.). With the demise of many communist regimes, and the gradual liberalization of the remainder towards capitalism, left-wing rhetoric can often move towards and merge with anarchistic thought.

- Anarchist: Anarchist groups are anti-authority or anti-government, and strongly support individual liberty and voluntary association of cooperative groups. Often blending anti-capitalism and populist or communist-like messages, modern anarchists tend to neglect the problem of what will replace the current form of government, but generally promote that small communities are the highest form of political organization necessary or desirable. Currently, anarchism is the ideology of choice for many individuals and

---

[103] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 198.

small groups who have no particular dedication to any ideology, and are looking for a convenient philosophy to justify their actions.

Religious

Religiously inspired terrorism is on the rise, with a forty-three percent increase of total international terror groups espousing religious motivation between 1980 and 1995.[104] While Islamic terrorists and organizations have been the most active, and the greatest recent threat to the United States, all of the major world religions have extremists that have taken up violence to further their perceived religious goals. Religiously motivated terrorists see their objectives as holy writ, and therefore infallible and non-negotiable.

Religious motivations can also be tied to ethnic and nationalist identities, such as Kashmiri separatists combining their desire to break away from India with the religious conflict between Islam and Hinduism. The conflict in Northern Ireland also provides an example of the mingling of religious identity with nationalist motivations. There are frequently instances where groups with the same general goal, such as Kashmiri independence, will engage in conflict over the nature of that goal (religious or secular government).

Christian, Jewish, Sikh, Hindu and a host of lesser known denominations have either seen activists commit terrorism in their name, or spawned cults professing adherence to the larger religion while following unique interpretations of that particular religion's dogma. Cults that adopt terrorism are often apocalyptic in their worldview, and are highly dangerous and unpredictable. It is interesting to note that religiously motivated terrorists are among the most energetic developers of Weapons of Mass Destruction (WMD) for terrorist use. Also, religiously inspired cults executed the first confirmed uses of biological and chemical nerve agents by terrorists.

Social

Often particular social policies or issues will be so contentious that they will incite extremist behavior and terrorism. Frequently this is referred to as "single issue" or "special interest" terrorism. Some issues that have produced terrorist activities in the United States and other countries are:

- Animal rights

- Abortion

- Ecology/environment

- Minority rights

> **"The overall threat posed by special interest extremism appears to be increasing."**
>
> From "Terrorism in the United States, 1999" FBI Publication #0308, Federal Bureau of Investigation

---

[104] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 90.

Location or Geographic Categories

Geographic designations have been used in the past, and although they are often confusing, and even irrelevant when referring to international and transnational terrorism, they still appear. Often, a geographical association to the area with which the group is primarily concerned will be made. "Mid-Eastern" is an example of this category, and came into use as a popular shorthand label for Palestinian and Arab groups in the 1970s and early 1980s. Frequently, these designations are only relevant to the government or state that uses them. However, when tied to particular regions or states, the concepts of <u>domestic</u> and <u>international</u> terrorism can be useful.

- *Domestic* or *Indigenous.* These terrorists are "home-grown" and operate within and against their home country. They are frequently tied to extreme social or political factions within a particular society, and focus their efforts specifically on their nation's socio-political arena.

- *International* or *Transnational.* Often describing the support and operational reach of a group, these terms are often loosely defined, and can be applied to widely different capabilities.

  - International groups typically operate in multiple countries, but retain a geographic focus for their activities. Hizballah, for example, has cells worldwide, and has conducted operations in multiple countries, but is primarily concerned with events in Lebanon and Israel.

  - Transnational groups operate internationally, but are not tied to a particular country, or even region. Al Qaeda is transnational; being made up of many nationalities, having been based out of multiple countries simultaneously, and conducting operations throughout the world. Their objectives affect dozens of countries with differing political systems, religions, ethnic compositions, and national interests.

An insurgency-linked terrorist group that routinely crosses an international border to conduct attacks, and then flees to safe haven in a neighboring country, is "international" in the strict sense of the word, but does not compare to groups that habitually operate across regions and continents.

Section III: Knowledge Exchange and Proliferation Between Organizations

Terrorist groups increase their capabilities through the exchange of knowledge. These exchanges occur both directly and indirectly. Direct exchange occurs when one group provides the other with training or experienced personnel not readily available otherwise. An example of direct exchange is the provision of sophisticated bomb construction expertise by the IRA and ETA to less experienced groups. In 2001, three members associated with the IRA were arrested in Colombia. Traveling on false passports and with traces of explosives on their clothes and luggage,[105] the three individuals appeared to

---

[105] Rachael Ehrenfeld, *IRA + PLO + Terror* [journal on-line] American Center for Democracy (ACD), 21 August 2002; available from http://public-integrity.org/publications21.htm; Internet; accessed 13 February 2004.

be an instance of inter-group terrorist support in use of explosives and other terrorist techniques. U.S. government reports state an IRA and FARC connection since at least 1998 with multiple visits of IRA operatives to Colombia. Terrorism techniques not previously observed as a norm in FARC operations, such as use of secondary explosive devices, indicate a transfer of IRA techniques.[106]

In order to disseminate much of this knowledge, terrorist organizations often develop extensive training initiatives. Al Qaeda, for instance, has assembled in excess of 10,000 pages of written training material, more than 100 hours of training videos, and a global network of training camps.[107] This training material can be distributed in both hard copy or via the Internet.

Indirect transfer of knowledge occurs when one group carries out a successful operation and is studied and emulated by others. The explosion of hijacking operations in the 1970s, and the similar proliferation of hostage taking in the 1980s were the result of terrorist groups observing and emulating successful techniques. However, this type of knowledge transfer is not restricted to just violent international terrorist groups. The same is true for many of the single-issue groups located in the United States. The Stop Huntingdon Animal Cruelty (SHAC) group uses tactics initially used by British activists, which targets the homes of individuals that are related in some form to Huntingdon Life Sciences, an animal-testing lab. They use tactics just short of physical violence in terrorizing families and entire neighborhoods, such as showing up with sirens and bullhorns at 3 a.m., plastering the neighborhood with photographs of mutilated dogs, and posting home and work phone numbers on the Internet. An Oregon-based watchdog group, Stop Eco-Violence, stated that they are seeing a copycat effect within the eco-terror movement, with other groups now using the same tactics.[108]

These examples of knowledge exchange highlight the fact that assessments of terrorist threat capabilities cannot only be based upon proven operational abilities. Military professionals must evaluate potential terrorist threats according to what capabilities they may acquire through known or suspected associations with other groups. Also, consideration must be given to capabilities that can reasonably be acquired through the study and employment of techniques and approaches that have proven successful for other terrorist organizations.

A development related to this is the proliferation of specialized knowledge useful to terrorists over the last decade. The reductions in military and intelligence establishments after the Cold War have made expertise in sabotage, espionage, small unit tactics, and other useful skills readily available. Similar reductions in research and development institutions make technical and scientific expertise in weapons of mass destruction, information technology, and electronic countermeasures more accessible, either through direct contacts or intermediaries such as rogue or dysfunctional states.

---

[106] Jan Schuurman, *Tourists or Terrorists?* [press review on-line] Radio Netherlands, 25 April 2002; available from http://www.rnw.nl/hotspots/html/irel020425.html; Internet; accessed 13 February 2004.

[107] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 7.

[108] Don Thompson, "British Ecoterror Tactics Spread to U.S. Activists," *The Mercury News*, 10 May 2003, 1-2; available from http://www.mercurynews.com/mld/mercurynews/news/local/5832723.htm?1c; Internet; accessed 21 April 2004.

Conclusion

This chapter provided descriptions of the common organizational models for terrorist groups. It also presented an array of categories and descriptions of terrorists and terrorist groups, in order to clarify the jargon that surrounds this topic, and to avoid those terms that are not useful for the purposes of military professionals assessing the terrorist threat.

Chapter 4
Assessing Terrorist Capabilities and Intentions

> **Everything was absolutely ideal on the day I bombed the Pentagon. The sky was blue. The birds were singing. And the bastards were finally going to get what was coming to them.**
>
> Bill Ayers, Former Weather Underground leader in his memoir *Fugitive Days*

This chapter examines the nature of the terrorist threat to U.S. military forces. Principal themes focus on the following aspects:

- Understand who will want to engage U.S. military forces utilizing terror tactics, and why attacking military targets would be desirable.

- Explore why particular U.S. forces would be targeted, and how that targeting is accomplished against U.S. forces.

- Provide context by categorizing U.S. forces based upon their status as Deployed, Deployable, and Non-deployable elements.

- Clarify the categorization of various threats by categorizing terrorist groups by their functional capabilities.

When discussing terrorist attacks on "military targets," targets include individuals or facilities that are attacked because of their military identity. These type attacks include off duty personnel in civilian settings specifically attacked because of their status as military personnel. Normally, this does not address military personnel or activities that are victims of attacks directed at non-military targets.

In discussing questions of why terrorists will conduct particular activities, clarifying terminology should start with terrorist goals and objectives.

Objective: The standard definition of *objective* is – "The clearly defined, decisive, and attainable aims which every military operation should be directed towards."[109] For the purposes of this work, terrorist objectives will refer to the intended outcome or result of one or a series of terrorist operations or actions. It is analogous to the tactical or operational levels of war as described in FM 101-5-1.

Goals: The term *goals* will refer to the strategic end or end state that the terrorist objectives are intended to obtain. Terrorist organization goals equate to the strategic level of war as described in FM 101-5-1.

---

[109] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 9 June 2004.

The United States entered the twenty-first century as the single most influential nation in the world. The world perceives the United States as the sole remaining superpower, the victor of the Cold War. Some quarters view the United States as a hegemonic enforcer of its own brand of order and stability.[110] Because of this influence, anyone seeking to change the existing world order through aggression, coercion or violence sees the United States as an eventual adversary. As a result, they seek means to challenge the United States. Various forms of low intensity conflict, and competition and conflicts short of war are seen by most of America's potential adversaries as the most promising methods of presenting this challenge.[111] Terrorism is a component of these strategies.

With the end of the bi-polar world order and the demise of the Soviet Union, U.S. diplomatic, military, and economic interventions have become more frequent, and more significant. Because of this dominance, some antagonists see terrorism as the only effective means of competing with the United States. In terms of effectiveness, al Qaeda alone has killed more Americans with terrorist attacks than all of the casualties suffered in all the campaigns and interventions since 1980, including both Gulf Wars. The resulting effects on the United States have been immense, and the unprecedented response by the U.S. to the threat of terrorism encourages the belief that the asymmetric approach of terrorism is the only way of defeating the United States.

As part of the overall primacy of American power, United States military forces have demonstrated dominant conventional capabilities through successful campaigns and participation in multiple international interventions. Despite this level of preeminence, U.S. military forces remain vulnerable to terrorist operations.

There are concrete reasons to consider terrorism as a specific and pervasive risk for U.S. forces. Factors contributing to a greater danger of attack to military forces are:

- Some groups have actually identified the U.S. military as targets. Al Qaeda has specifically identified military targets as one of its two major priorities,[112] and the FARC has stated that any U.S. forces deployed in Colombia are considered targets.

- The improved protection or "hardening" of many non-military targets. Formerly, non-military targets were "softer" due to a lower degree of security consciousness and a lack of belief in a credible threat. Frequent attacks on non-military personnel and organizations, both government and corporate, have resulted in the imposition of improved security measures, greater threat awareness, and acceptance of increased expenditures for protection on many of these targets. This increase in the level of difficulty to the terrorist has reduced the bias toward non-military targets.

- The increasing exposure of forward deployed and internationally based military forces in "permissive areas" for terrorist activities. As of February 2004, the United States had

---

[110] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare,* trans. Department of State, American Embassy Beijing Staff Translators (Washington, D.C., 1999).
[111] Ibid., Part III.
[112] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 76.

military forces located in over 120 countries performing duties from combat operations, to peacekeeping, to training foreign militaries.[113] Clearly, increases in the operations tempo and the number of overseas deployments raise the odds that U.S. forces will operate in areas that are more accessible to terrorist groups than CONUS or established overseas bases. This is especially true when the potential military target may in fact come directly to the terrorist, operating in his stronghold due to mission requirements. Likewise, some countries where U.S. forces are permanently based have groups of domestic terrorists that would not be a threat outside that country, yet pose significant risk to units or individuals stationed there.

- The symbolic value of successful attacks against military targets has often been a consideration in terrorist planning. This is now particularly true of the U.S. military, widely perceived as the premiere military in the world. The primacy of the U.S. Department of Defense in the response to the September 11th attacks, and the operations in Afghanistan and Iraq further raises the profile of the U.S. military. Improved public perceptions about the military from the U.S. viewpoint increase their value as terror targets. To many regions, however, the U.S. member in the Armed Forces is a symbol of imperialism. Consequently, striking at a respected institution whose members have public sympathy at home, and who is perceived as a threat in many regions of the world, and who constitutes a direct threat to terrorist groups will become highly attractive. The potential status and psychological impact of such a coup is a strong inducement to all types of terrorist groups. Additionally, terrorist groups recognize that even relatively small losses of military forces from terrorist attacks receive extensive media coverage and can destroy popular and political support for military operations by Western governments.[114]

- The aims and methods of terrorists – particularly religious extremists – have grown more radical, innovative and difficult to predict. A generational change in leadership can have varied outcomes. In some cases, more destruction may result; in other cases, organizations may simply lose their cohesion and cease to be a significant influence. Added to this is the effect of extended periods of turmoil and conflict in many regions of the world for the past two decades. This provides recruits and followers that have been desensitized to violence, and who have known nothing but conflict and insecurity for all of their lives. As noted in *Jihad: The Trail of Political Islam*, "The dispersion all over the world, after 1992, of the jihadist-salafists formerly concentrated in Kabul [Afghanistan] and Peshawar [Pakistan], more than anything else, explains the sudden, lightning expansion of radical Islamism in Muslim countries and the West."[115]

---

[113] "Where are the Legions? [SPQR] Global Deployments of US Forces," Global Security.org, 16 April 2004, 1; available from http://www.globalsecurity.org/military/ops/global-deployments.htm; Internet; accessed 21 April 2004.

[114] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 77.

[115] Gilles Kepel, *Jihad: The Trail of Political Islam* (Cambridge: The Belknap Press of Harvard University Press): 299.

Section I: Potential Adversaries and Their Motivations

Potential Adversaries

There are a large number of terrorist organizations active in the world today, and a wide variety of them are potential antagonists willing to attack U.S. military forces throughout the world. Some of these groups, such as al Qaeda are transnational in nature, whereas others such as the Revolutionary Armed Forces of Colombia (FARC) are more regionally focused. However, in both cases, they have identified the U.S. military as potential targets. Appendix A contains a listing of specific terrorist groups and their operational range. The threat environment for terrorism is too dynamic to discuss specific groups or individuals in this context, but identifying situations that may exacerbate or trigger the motivations of potential adversaries can assist in developing some idea of whose interests are served by such attacks.

- Presence – Many antagonists are opposed to the presence of U.S. military forces in a particular area, or the presence of organizations U.S. forces are safeguarding. Frequently, this opposition is because the U.S. presence is preventing particular political, military, or criminal activities, but it can also be culturally inspired. Another possibility is that the presence of U.S. forces is viewed as an opportunity to eliminate or dominate rival factions, and attacks on U.S. forces would be staged in the hopes that the U.S. would encourage the suppression or disarmament of rivals. Usama bin Laden is an excellent example of someone opposed to U.S presence in an area, i.e., the Arabian Peninsula. In particular, he sees the United States as invaders of the land of Islam by "occupying the territory of the Two Holy Places" (U.S. military bases in Saudi Arabia).

- Culture – Antagonists who are directly opposed to one or more major characteristics of American culture, such as capitalism, secular democracy, polytheism, pop culture, women's rights, sexual freedom, or racial tolerance; will attack Americans wherever found. Groups primarily motivated by cultural differences will not differentiate between civilian and military targets, other than in their respective degree of risk and difficulty to attack.

- State of Conflict – Groups that feel that they are "at war," or in a social or political conflict with the United States will target military personnel and facilities to gain legitimacy and make statements. Likewise, states that are engaged in or anticipate hostilities with the U.S. will use sponsored terrorist organizations or clandestine military or intelligence assets to attack military targets.[116]

In considering who may be our potential antagonists, several things must be kept in mind. While a "threat" is normally considered to be an actor with both the capability *and* intention to actively oppose the U.S.,[117] both these factors can shift rapidly when dealing with terrorist organizations.

Unit planners must evaluate all known and suspected terrorist groups in the area regardless of their previous attitude toward the U.S. and U.S. military. Terrorism is dynamic, and behavior

---

[116] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 52.
[117] FM 7-100, *Opposing Force Doctrinal Framework and Strategy*, May 2003.

patterns volatile. Groups that are neutral or that avoided targeting U.S. interests in the past can change their attitudes rapidly. Announced or perceived U.S. policy may antagonize previously neutral groups, if that policy conflicts with the goals or objectives of the group. Changes in leadership or internal fractionalization of a group may cause changes in targeting policies or priorities. Also, any organization amoral enough to utilize terrorism as a tactic will not hesitate in exploiting an "ally" or partner if the benefits seem to warrant it. For all these reasons, assumptions regarding previous attitudes of terrorists toward targeting U.S. military assets should be reexamined frequently and with a highly critical mindset.

Also, in assessing potential antagonists, caution should be taken to avoid considering only those threats that are viewed as particularly large or well known. There is a popular tendency to allow the amount of media attention a group can command to determine how we perceive its effectiveness or lethality. Because of the nature of the modern news media, as well as the acknowledged skill of terrorist groups in manipulating it, this is an invalid approach. Small, little known groups, especially the "want-to-be" groups, can pose threats that are as probable as larger groups, and every bit as dangerous. This is particularly true when operating in a region or country not previously accustomed to a U.S. military presence, and where domestic or indigenous groups may suddenly be presented with the opportunity of gaining international attention through an attack on U.S. forces.

Motivations to Attack U.S. Forces

During the post-colonial and nationalist insurgencies of the Cold War, terrorists often contended that one civilian casualty was worth many enemy military dead. This was due to the fact that many insurgencies had simultaneous military and terror campaigns, so the novelty and impact of military casualties was lessened.[118] Even when not involved in hostilities, military casualties delivered less psychological impact because of expectations that military personnel are "at-risk" due to their profession. Terrorists also pursue soft targets, preferring unarmed, less secure victims. A saying attributed to any number of terrorists is "Why hunt wolves when there are so many sheep about?" While there are exceptions to this, such as the consistent targeting of British soldiers and police by the IRA, targeting civilians was the clearly preferred tactic.

> **"One corpse in a [suit] jacket is always worth more than twenty in uniform. "**
> Ramdane Abane, Senior FLN Terrorist Leader

As terrorism became less and less associated with classical insurgencies and more international in scope, the preference for civilian targets became less pronounced. American military installations and personnel were frequently targeted in the 1980s and 1990s by anti-NATO European terrorists, and by state sponsored terrorists acting on behalf of a variety of regimes.[119] These attacks generally struck at military targets that were not engaged in hostilities, but that were accessible to the terrorists due to their being based or deployed overseas. This trend has accelerated, although the focus has shifted from Europe to the Persian Gulf region.

---

[118] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 61.
[119] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Chronology of Terrorist Events."

There are two strategic factors in terrorists accepting the greater risks associated with attacking military targets: accessibility and symbolic value.

- Accessibility – Military forces are often based or deployed into areas that are "permissive" to terrorist operations. These environments need not be destabilized regions or failed and dysfunctional states such as Bosnia, Lebanon or Somalia, but can also be functioning states with liberal laws, permissive border controls, and existing terrorist infrastructures.

- Symbolic Value – For the United States, commitment of military forces is a significant indicator of national interest, and carries major political consequences. Targeting military forces so committed can achieve a greater visibility and significance than targeting existing civilian targets such as diplomats or commercial personnel and facilities. Additionally, the very presence of U.S. forces in some regions, allegedly offending political or religious sensibilities, can be presented as a justification for the attack.

Section II: Considerations in Targeting U.S. Forces

A principal consideration in terrorist targeting is the psychological impact on the selected audience. U.S. forces whose destruction or damage would provide a psychological impact that serves the goals of the terrorist are therefore at risk. However, a key point must be understood; assessment of the risk to potential targets must focus less on their military value, and more on their value to the terrorist in terms of psychological impact.

Risk Assessment

U.S. military risk assessment normally looks at what is most militarily valuable (mission essential) to us. Operationally vital systems and equipment, or key personnel are assumed to be at greater risk based upon an estimation of their military worth in particular conditions. However, the benefits for a terrorist organization do not lie in defeating our military aims. A terrorist may view value as a function of the overall psychological impact that destruction of a target will have on a population, as well as the cascading physical effects of damaging or destroying a critical piece or aspect of an organization or infrastructure. The loss of a single piece of equipment (such as an artillery targeting radar) has important military impact, but little psychological impact outside the unit or organization that relies on it. For a terrorist, expending assets to destroy such a piece of equipment would not make sense unless it were tied to some other event or objective.

As an example, consider a hypothetical comparison of the relative worth of two task forces as terrorist targets. One is a task force built upon a divisional cavalry squadron, soon to play a critical tactical role in a conventional campaign during a major regional conflict. The other is a Civil Affairs (CA) task force TACON to the same division during this conflict. With an upcoming conventional combat mission, the immediate military value of the cavalry task force is relatively greater, and conventionally considered subject to greater risk.

However, from the terrorist perspective, the CA task force is the better target. The composition, mission, and nature of the combat unit render it more difficult to strike, less susceptible to casualties, and capable of controlling the release of information regarding

casualties and effects that comprise the terrorist ability to exploit any attack (see Appendix B as regards to the exploitation phase of terrorist operations). The CA unit will be more exposed because of its mission requirements to operate closer to likely terrorist operational environments (population centers). It is less capable of self-defense and the CA unit is likely to contain more suitable victims from the terrorist point of view; reservists, female soldiers, soldiers with a family. All of these categories have a greater likelihood of psychological impact than the average member of a combat unit, and therefore a higher target value for terrorist purposes. Additionally, because of its requirement to interact with the local population, the CA task force is less likely to prevent external knowledge of an attack and its effects, which makes exploitation of the attack easier. Finally, a terrorist may want to maintain instability in an area to enhance organizational objectives within a civilian population. Countering pacification or other civil affairs missions is a logical aspect of reinforcing an unstable situation.

From a terrorist's perspective, targeting individual soldiers, especially those that are not perceived to be in imminent danger or engaged in hostilities, is very effective. Several soldiers kidnapped and gruesomely murdered would have a small overall military impact, but a potentially huge psychological payoff for the terrorist. With the atrocity recorded as digital video and streamed via multiple sources on the Internet to bypass any self-censorship news networks might exercise, it would be accessible throughout the world. Palestinian groups have conducted this tactic with varying degrees of success against Israeli soldiers and various terrorist groups have used it against American civilians.

Consider the amount of media attention given the abduction and eventual murder of reporter Daniel Pearl in 2001, and how the video of his murder was nearly presented on cable television networks. Use of this tactic continued in 2004 when two Americans were kidnapped and beheaded by terrorists. Nicholas Berg was an American businessman seeking telecommunications work in Iraq when he was kidnapped and beheaded in May 2004. Another American, Paul Johnson who worked for Lockheed Martin in Saudi Arabia, was kidnapped and beheaded in June 2004. In both cases, the terrorists disseminated videos (Berg) and pictures (Johnson) of the beheadings over the Internet.

Undoubtedly, the technique used in the three murders discussed above would be effective even if soldiers were the victims. As a society, Americans value every life. Terrorists understand this American trait, and as stated in Chapter 2, view our aversion to casualties as a vulnerability. A case in point occurred during the air campaign against Serbia in the spring of 1999. Three U.S. Army soldiers patrolling the Yugoslav-Macedonian border during this period became separated from a larger patrol and were captured by the Serbians. Serbian President Slobodan Milosevic orchestrated an international media campaign during the capture and month long captivity of the three. Maintaining an ambiguous stance on the status of the prisoners, and their possible fate, Milosevic eventually scored a coup by releasing the three to an unofficial mission of prominent American political figures, resulting in even more media coverage. In this case, the political and psychological impact far outweighed any operational impact caused by the capture of three soldiers and one vehicle. While Milosevic enjoyed some advantages as a head of state that few terrorist organizations will possess, proper media manipulation can make up this deficiency.

The media and sensational incidents can acquire a life of their own as reports and speculations sometimes create an event far beyond the actual incident. Although not terrorist related, the 2003 publicity surrounding the wartime capture, rescue, and subsequent medical rehabilitation of U.S. soldier Jessica Lynch quickly erupted as a major storyline and continued to stage headlines for months after the combat action. Months later, she was still receiving national and international news coverage on particular aspects of the capture.[120]

Reasons for Targeting

With the variety of terrorist motivations and goals, the reasons to target U.S. military units or individual personnel are equally varied. The most common motivations in recent history are discussed below.

Demonstration of Capability

This is a method to demonstrate a group's ability to deliver on its threats, and to establish a level of effectiveness as a future threat. Targets may be selected for either military or symbolic value, but the true intent is to show that the terrorist has the capability to negate a U.S. military advantage and concurrently promote their organizational agenda. Senior military officials are often a target. The Red Army Faction (RAF) conducted numerous terrorist activities against military presence in Germany and countries of the North Atlantic Treaty Organization (NATO) in the 1970s and 1980s. Shifting from goals for a complete revolution of German society, the RAF concentrated much of their capabilities on a campaign to reduce NATO and U.S. military presence in Germany as a way to possibly build a more sympathetic understanding for societal change in Germany.[121]

In 1979, the RAF attempted to assassinate General Alexander Haig, the Supreme Allied Commander in Europe and NATO. A remotely controlled bomb had been placed in a road culvert near Casteau, Belgium that was used frequently by General Haig. A detonator of nine-volt batteries and a household switch connected the bomb via 500 feet of wire that was camouflaged by earth and grass. The blast lifted the general's car into the air and damaged the accompanying security vehicle; three guards in the security vehicle were lightly injured.[122]

In 1981, General Frederick Kroesen and his wife were slightly injured when their car was attacked by terrorists, believed to be associated with the RAF, with rocket propelled grenades and gunfire. The assassination attempt occurred near Heidelberg, Germany, as the general was enroute to his headquarters as the Commander in Chief of United States Army Europe and Commander of NATO's Central Army Group. One site about 200 yards from the target point evidenced terrorist surveillance activity with an abandoned tent, radio transmitter, sleeping bag, and food.[123] Fortunately the terrorists failed in their attempts to assassinate

---

[120] "Too Painful" *ABC News* [news on-line] 11 November, 2003; available from http://abcnews.go.com/sections/Primetime/US/Jessica_Lynch_031106-1.html; Internet; accessed 12 February 2004.

[121] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 49-51.

[122] John Vinocur, *"Bomb Attempt on Gen. Haig's Life Not Tied to Major Terrorist Groups,"* New York Times, 27 June 1979, p. A13.

[123] John Vinocur, *"U.S. General Safe in Raid in Germany,"* New York Times. 16 September 1981, p. A1.

General Kroesen and General Haig; however, these attacks are examples of terrorist groups demonstrating their capabilities to deliver on their threats.

A more recent and more successful example is the Khobar Towers attack in Saudi Arabia. To Islamic fundamentalists, the presence of U.S. military forces in Saudi Arabia is considered particularly offensive due to the religious importance of the Saudi city of Mecca. In June of 1996, a housing facility for U.S. Air Force personnel near Dhahran, Saudi Arabia was attacked with a large truck bomb. The Khobar Towers attack killed nineteen U.S. Air Force personnel and wounded about 400 other U.S. military members,[124] and demonstrated terrorist ability to back up threats with effective action. Members of Saudi Hizballah, a member of Lebanese Hizballah, and an unnamed Iranian were indicted by the U.S. Department of Justice for this act of terrorism. On the heels of this attack, terrorists declared war on American forces in the Persian Gulf region in August 1996, and announced that all U.S. forces must be withdrawn, or suffer further attacks.

Influence U.S. Policy

Terrorists can attack military forces with the intent to force a change in U.S. policy. Hizballah and their Syrian sponsors were concerned that the deployment of international peacekeeping forces into Lebanon in the spring of 1983 would reduce their freedom of action in the ongoing Lebanese Civil War. Near-simultaneous suicide truck bomb attacks on the U.S. Marine and French paratroop barracks in October of 1983 killed 241 U.S. servicemen, and 60 French paratroopers. Combined with an earlier bombing campaign against the embassies of the U.S. and other countries, these attacks resulted in the withdrawal of the international military force.

Figure 4-1. **U.S. Marine Barracks, Beirut**
(*Source*: USMC Photo)

Domestic Politics

The desire to discredit U.S. Federal, state, and local governments can result in military units and personnel being targeted by domestic groups. Anti-war extremist groups targeted ROTC detachments, draft board offices, and university facilities involved in military research during the Vietnam War.[125] The Weather Underground likewise targeted recruiting offices in the late 70's. Both of these campaigns were undertaken to influence U.S. domestic politics. In more recent times, various anti-government groups have targeted CONUS military bases believing them to be staging areas for United Nations directed foreign military forces. During the twenty-year period from 1980 to 1999 (inclusive), thirteen specifically domestic military

---

[124] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 71.

[125] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Student Terror: The Weathermen "

targets were struck by terrorist activity. This does not count military facilities or personnel who were collocated in the other 101 U.S. Government targets that were attacked.[126]

Reduce Military Capability

Military forces can be targeted to reduce or remove a specific capability or impair effectiveness. Killing one key or very effective individual can also reduce the motivation for others to accept responsible positions or perform above the norm, and thereby risk becoming targets. This tactic will usually be combined with some symbolic justification, such as "justice" applied by the terrorists because of alleged "war crimes" perpetrated by the victim.

The assassination of Colonel Nick Rowe in Manila provides a good example of this. Colonel Rowe was in charge of the Joint U.S. Military Assistance Group for the Philippines. His two years there had been spent contributing to the improvement of the Philippine Army's counterinsurgency capability, and the insurgent New People's Army (NPA) felt he was doing his job too well. He was assassinated in April of 1989 in a moving ambush where small arms fire defeated the protection of his armored official vehicle. The NPA announced that the reason for the assassination was Colonel Rowe's notable Vietnam service record. The NPA hoped this would draw the parallel that the Philippines were becoming "another Vietnam." This justification was not stressed at the time, and seems to have been of much less importance to the NPA than the elimination of the threat posed by Colonel Rowe's activities.[127]

Prevent or Delay Deployment

During Operation Desert Shield, Saddam Hussein called for terrorist activity to be directed against the countries of the coalition preparing to invade Iraq. Attacks conducted by indigenous terrorist groups Dev Sol and 17 November took place against U.S. staging areas in Turkey and Greece. Iraq directly supported these overseas attacks with weapons components delivered via diplomatic pouch and other assistance.[128] Although Saddam Hussein did not have the influence to convince or compel a larger Mideast surge in terrorism, terrorist activities in general did increase during the period of the air campaign and subsequent invasion of Iraq, totaling 275 incidents.[129] Due to extensive counter-terrorism efforts and international coordination, the overall effort to disrupt coalition deployments was ineffective. However, this period is a vivid example of the threat that both deployed and deploying units may face in the future. As a comparison of the 275 incidents in the relatively limited Gulf War period, only 274[130] incidents were recorded for the entire year of 1998.

---

[126] Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999,* Report 0308, (Washington, D.C., n.d.), 53.

[127] *Colonel James "Nick" Rowe* (Psychological Operations Web Site, n.d.); available at http://www.psywarrior.com/ rowe.html; Internet; accessed 7 January 2003.

[128] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 52.

[129] Ibid., 52.

[130] Department of State, *Patterns of Global Terrorism 2003* (Washington, D.C., April 2004; revised 22 June 2004), 176.

In addition to terrorist activities outside Iraq, the Iraqi government conducted what amounted to the largest hostage taking in modern time. They seized 10,000 Kuwaiti citizens, and hundreds of foreigners resident in Iraq, as "human shields" immediately after the start of Operation Desert Shield and during preparations for the liberation of Kuwait. Fortunately, most of the hostages were released before the initiation of Desert Storm.[131]

Other terrorist incidents indicate the potential for disrupting deployments or materiel in transit. The tensions of political, environmental, and economic impacts add to the specific damage or destruction of an incident. The terrorist suicide boat bombing in 2002 of the French tanker ship *Limburg* near Ash Shihr and east of Aden spilled 90,000 barrels of oil into the ocean and contaminated 45 miles of coastline.[132] One immediate economic impact of this small boat and TNT detonation next to the *Limburg* was a maritime insurance increase in rates that tripled in the Yemeni area.[133] Another incident involved the suicide boat bombing of the USS *Cole* in 2000 while the ship was moored at a refueling point in Aden, Yemen. Terrorists exploited access control measures and perimeter security vulnerabilities of waterside approaches to the naval ship while near the coastline. The result, besides the international media attention, was 17 sailors killed, 42 crewmembers wounded, as well as extensive damage to the ship.[134] In more recent military operations, during the preparation for and conduct of Operation Iraqi Freedom, threat of terrorist attacks contributed to decisions by Turkey that significantly limited U.S. use of Turkish territory, facilities, and materiel.

Section III: Categorizing Terrorist Groups by Capability

> **"Asymmetric challenges can arise across the spectrum of conflict that will confront US forces in a theater of operations *or on US soil*."**
>
> "Global Trends 2015: A Dialogue About the Future With Nongovernment Experts" report (December 2000).

As discussed in Chapter 3, there are many different terms and labels used to describe terrorist organizations. Most of these terms provide little or no information of value to the military professional in assessing the true threat of a terrorist group as an adversary. For the unit at

---

[131] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Chronology of Terrorist Events."

[132] *"Evidence Points to Yemen Terror Attack,"* CBS News.com [database on-line]; available from http://www.cbsnews.com/stories/2002/10/06/world/main524488.shtml; Internet; accessed 21 January 2004.

[133] *"The Terrorism Maritime Threat,"* United Press International 2 December 2003 [Militarycom database on-line]; Internet; accessed 21 January 2004; and, *"French Tanker Explosion Confirmed as Terror Attack,"* [database on-line]; available from http://www.ict.org.il/spotlight/det.cfm?id=837; Internet; accessed 21 January 2004.

[134] *Statement Before the 107th [U.S.] Congress, Chairman of the Joint Chiefs of Staff*, Senate Armed Services Committee May 3, 2001; [database on-line] available from http://www.dtic.mil/jcs/chairman/3MAY01_SASC_CJCS.htm; Internet; accessed 18 February 2004.

risk of terrorist attack, it is important to understand the capabilities the groups have that can be employed against the military unit.

In this section we will discuss a method to assist armed forces personnel in the rapid and clear assessment and comparison of terrorist threats based upon militarily relevant criteria. It is designed to help describe terror groups by their capabilities to target and attack U.S. military forces, rather than by legal status, political or religious characteristics, or other value-based criteria. Capability-driven group descriptions are desirable for a variety of reasons.

Capabilities Descriptions are Neutral: Terms describing capabilities are less likely to be emotionally charged. Attaching politically or socially relevant descriptions to a group allows value judgments to be made relative to those terms. Also, like legal categories and other methods of classifying terrorists, they do not contain much useful information for leaders and planners.

Capability Descriptions do not Constrain: Accepting descriptions that focus on ideological or religious motivations for terrorist groups can be misleading, and encourage false assumptions. Ideological considerations do play a part in determining if a group will target U.S. forces, but they have no effect on that group's capability to do so. Any group can become a threat because it's announced objectives or ideology can change or are misleading, perhaps even unimportant.[135] Also, changes to the political situation, U.S. policy, or the role or mission of U.S. forces may cause formerly neutral or ideologically allied groups to become hostile.

A relatively recent example is Afghanistan following the 1979 Soviet intervention. Initially, the United States provided massive aid to help the Afghan resistance after the Soviets invaded in December of 1979. Many of these Afghan fighters confronted the Soviets as a corrupting Western influence and the fatwas issued by the ulemas interpreted the Soviet intervention as an invasion of the territory of Islam by the impious. However, these same fighters willingly accepted Western aid in fighting the Soviet occupation. Perceptions of both the United States and the mujahedeen changed, though, following the defeat of the Soviets. After the Soviets withdrew in 1989, the Afghan cause lost some of its strategic importance and the U.S. changed its view on its support to these "freedom fighters." Washington reduced financial support, and the U.S. Congress became concerned with the drug trade and involvement by mujahedeen leaders. Consequently, these mujahedeen leaders were classified as extremists and the supply of U.S. arms stopped.[136] From the viewpoint of the mujahedeen, they had defeated the Soviets and seemed to forget the support they received from the United States. Many of these jihad veterans became followers of a new breed of Islamist ideology, jihadist-salafism, whose perception of the world involved religious doctrine and armed violence and whose first doctrinal principle was to rationalize the existence and behavior of militants. Although their anti-Western sentiment was set aside while the United States supported them in their jihad against the Soviets, this attitude

---

[135] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 31-35.
[136] Gilles Kepel, *Jihad: The Trail of Political Islam* (Cambridge: The Belknap Press of Harvard University Press): 136-150.

returned after the Soviets withdrew and their primary target became the United States, who was perceived as the greatest enemy of the faith.[137]

Measures of Capability are Militarily Pertinent: Most systems used to classify terrorists are militarily irrelevant. For the most part, knowing the legal status, social orientation, or political theory of a potential truck bomber is of less value than knowing what sort of explosive devices he can afford, where in the operational area he can strike, and what level of local support and sympathizers he can expect. Motivations and behaviors are important to long term terror and counter-terror strategies, but play a minor role in the tactical activities of terrorists and the true threat opposing our forces.

Specific Measures of Capability

In describing the capabilities of a terrorist group, simple, measurable, concrete terms have been selected for use. These are the objective, levels of support, training, and operational presence of a particular group. These factors drive the capabilities of a terrorist organization, not the ideology, religion, or status as determined by U.S. legislation or UN resolution. This method is not intended to add another layer of nomenclature to an already thick coat that covers terrorism analysis. It is designed to be a method by which unit leaders and planners can organize pertinent, objective data about potential threats. This data must be researched or obtained from available intelligence information on specific threats within the AOR (Area Of Responsibility) as the unit prepares to conduct operations.

Objective

As defined in the introduction of this chapter this measure identifies the tactical intent and the operational priorities of an organization. It is the actual directing principle(s) behind group activities. By determining what the group wishes to accomplish, the likelihood and circumstances under which that group would target U.S. forces or facilities can be determined.

The objective may be derived from both communications of the organization and the actions it undertakes. Group communications must be examined with a critical eye toward the use of rhetoric and dogma. As mentioned in Chapter 2, ideological material may be unimportant to the actual objectives of a group. Actual indicators in terrorist communiqués are likely to be: what potential targets are concretely threatened and what organizations or individuals are identified with negative concepts or de-humanizing language. A group may declare itself to be "anti-colonialist", but in fact ignore targets associated with a nation that has colonies, and associate "colonialism" with another organization such as NATO, which they intend to target.

A 2004 training publication by al Qaeda is an excellent illustration of organizational communications transmitting the objectives of the group. In March 2004, al Qaeda released new targeting guidance to its members and other jihad groups around the world. The guidance was in a 9-page article called "The Targets Inside the Cities" and focused on urban targets. The document listed the various categories of targets, the rationale for striking them,

---

[137] Ibid., 218-220.

and examples of targets within each category. It also explained the advantages of conducting operations against cities, as well as the disadvantages. [138]

Support

There are several types of support that provides information about a terrorist group's capabilities. These are measures of the strength of financial, political, and popular support for a group, as well as the number of personnel and sympathizers it has. These factors indicate an organization's abilities to conduct and sustain operations, gather intelligence, seek sanctuary and exploit the results of operations.

- Financial: Is the organization well funded? Money is probably the greatest "force multiplier" of terrorist capabilities, and a well financed group can trade money for virtually any imaginable object or ability that their objectives require, especially weapons and equipment (discussed below). Financial support is a question of both income and expenditures. Many of the nationalist terror groups of significant durability (IRA, Hizballah) have incredibly large budgets, but they also have the infrastructure costs and political or social support obligations that come with building an alternative government or social structure.

  HAMAS is an example of a terrorist organization that has strong financial backing. Although the actual amount of money available to HAMAS is difficult to determine, estimates are that they receive several tens of millions of dollars per year. Sources for their funding includes unofficial sources in Saudi Arabia and the Gulf states, including approximately $3 million per year from Iran. They also receive funds from several charities and from some profitable economic projects.[139]

- Political: Does the organization have political sponsors or representation, either within international, state, or sub-state political bodies? This measures the degree to which a group is state sponsored or supported. It also considers whether the organization has its own political representatives or party that supports its aims (if not its methods). Political support blurs the lines between terrorism and other forms of conflict, and can generate sympathy and reduce negative consequences.

  Iran is probably the most active state supporter of terrorism. As reported in the State Department's 2002 *Patterns of Global Terrorism*, Iran provided Hizballah and several Palestinian rejectionist groups, including HAMAS, the Palestine Islamic Jihad, and the Popular Front for the Liberation of Palestine-General Command, with funding, safehaven, training, and weapons.[140]

---

[138] Ben N. Venzke, *al-Qaeda Targeting Guidance* – Version 1.0 (Alexandria, VA: IntelCenter/Tempest Publishing, LLC, 2004), 3-11.

[139] "Hamas," International Policy Institute for Counter-Terrorism, Profiles of International Terrorist Organizations, n.d., 5-6; available from http://www.ict.org.il/inter_ter/orgdet.cfm?orgid=13; Internet; accessed 26 April 2004.

[140] Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2002* (Washington, D.C., April 2003), 77.

- Popular: Popular support is the level of sympathy and passive or active support for the organization among populations it affects to represent, or operates within. Support from a constituency increases the effectiveness of other types of support. It makes funds go farther, and increases the legitimacy and visibility of a group. Popular support from populations the terrorists operate within reduces the security risks, and complicates the tasks of detection and defeat for the security forces.

  The United Self-Defense Forces of Colombia, or AUC, is an example of a terrorist organization with strong popular support. Its leaders reported that between 2002 and 2003, AUC strength grew from 8,000 to 14,000 combatants. Once backed mostly by wealthy business and ranching interests and former military leaders, it is receiving increasing support from poor Colombians.[141]

- The number of personnel and sympathizers: These are the actual workers and operators for the group, both active and "sleeper." This bears more upon the number of operations a group may undertake than the type of operations. The size of a group in terms of the number of personnel is important, but less so than other aspects of support. A small, well-funded, highly trained group may effectively attack targets in CONUS, whereas a larger, poorly funded, untrained group may be no direct threat to U.S. targets other than those in immediate proximity to its base area of operations. For instance, the Japanese Red Army (JRA) conducted numerous attacks around the world in the 1970s, including an attempted takeover of the U.S. Embassy in Kuala Lumpur. In 1988, the JRA was suspected of bombing a USO club in Naples, where 5 people were killed, including a U.S. servicewoman. Concurrent with this attack in Naples, a JRA operative was arrested with explosives on the New Jersey Turnpike, apparently planning an attack to coincide with the attack of the USO. Although the JRA conducted attacks around the world, the JRA only has six hard-core members, and at its peak, only had 30-40 members.[142]

Training

Training is the level of proficiency with tactics, techniques, technology and weapons useful to terrorist operations. It measures the abilities of a group in terms of specific operations and activities that threaten friendly forces. Keep in mind that innovative application of tactics can render moderately innocuous activities threatening. For example, the ability to stage a peaceful demonstration may be used to set the conditions for a riot that will provide cover for sniper assassinations of responding security forces.

The proliferation of expertise and technology has enabled groups that do not possess particular skills to obtain them relatively rapidly. In addition to the number of terrorists and terror groups that are willing and available to exchange training with one another, there are also experts in the technical, scientific, operational, and intelligence fields willing to provide training or augment operational capabilities for the right price.

---

[141] Scott Wilson, "A Transfer of Power in Colombia: Paramilitary's Rise Unintended Outcome of U.S. Assistance," *Washington Post Foreign Service,* 27 December 2001, 2; available from http://www.colhrnet.igc.org/newitems/may02/wp_transfer_power_27dec01.htm; Internet; accessed 26 April 2004.

[142] Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2002* (Washington, D.C., April 2003), 137.

Al Qaeda is well known for its extensive training. They have assembled thousands of pages of written training material and hundreds of hours of training videos. Training tapes have shown al Qaeda operatives conducting live fire exercises for a number of scenarios. These scenarios include assassinations, kidnappings, bombings, and small unit raids on various types of targets. Additionally, they conduct detailed planning, diagramming, and walk-through rehearsals prior to the actual live-fire exercise.

In the technology area, Aum Shinrikyo, has demonstrated its ability with chemicals and biological agents. It's most notable terrorist action was the release of sarin gas in five different subway trains in Tokyo in March 1995. However, it had released sarin previously in a Matsumoto residential area in June 1994. The cult has also cultured and experimented with numerous biological agents, to include botulin toxin, anthrax, cholera, and Q fever. Fortunately they were unsuccessful.[143]

Operational Presence

This indicates where a group can operate, and what limits there are to expansion of its operational area. It considers the physical locations of a group's assets, and the capability to move and conduct activities beyond those locations. Although the physical presence of group members is an important factor for determining operational presence, it must be noted that a terrorist cell can have a variety of functions, and not all cells have direct action capability. Many terrorist organizations have extensive support networks within the continental United States, but have not developed an operational capability to match. Their infrastructure within the U.S. is designed primarily to acquire funding and equipment. Yet they could contribute to a rapid expansion of operational capability into the U.S. if required.

For most groups today, their operational presence is determined by their strategic goals, operational objectives, and funding levels, rather than by physical constraints such as geographical distance. Terrorists have exploited the increasing economic, information, and transportation linkages around the globe to expand their presence. The tools available to terrorists to defeat travel controls include support or sponsorship from rogue states, alliances with criminal trafficking and smuggling networks, technologically enhanced forging operations, and simple bribery.

Weapons and Equipment

The weaponry and equipment available is an important part of any capabilities assessment of organizations that use violence. A separate measure of these categories has not been included in our measures above due to the rapidity of change in this area, and the relation of weapons and equipment capabilities to financial strength. Whereas conventional military organizations rely upon standardization, and often have the problem of "legacy" systems that must be used in lieu of the most modern technologies, terrorists rely upon weapons and equipment tailored to each new operational requirement. If a 30-year old RPG-7 will do the job, it will be used. If not, an appropriate system will be purchased. Since terrorists do not have to go through

---

[143] Kyle B. Olson, "Aum Shinrikyo: Once and Future Threat?" *Emerging Infectious Diseases*, no. 4 (July-August 1999): 513-514.

long acquisition processes like conventional militaries, their only limitation in obtaining state-of-the-art systems is financing, availability of the equipment, and training.

Terrorists use a broad range of weapons. Virtually any type of firearm can be employed, plus a wide variety of improvised explosive devices and conventional military munitions that are adapted for use for specific operational requirements. Additionally, some terrorists have employed both chemical and biological agents. Appendices D-G are provided as an introduction to various types of terrorist weaponry and their attack capabilities.

Proxies

Terrorist capabilities are solely a function of the individual group or organization. As previously mentioned, many groups maintain links to rogue states, criminal gangs, activist groups, and other organizations that can expand their capabilities. This expansion may exceed the traditional areas of training and logistic assistance. It can include the actual conduct of operations, with one group acting as a proxy for the other. This is extremely dangerous, as it grafts the motivation and objectives of the group requesting an operation onto the capabilities and characteristics of the organization executing the operation.

Revolutionary groups such as the Baader-Meinhof Gang and the JRA provided operational personnel or undertook specific missions for Palestinian groups in the 1970s in exchange for training and support. Iraqi efforts to instigate terrorist activities as part of their strategy during the Gulf War[144] have been mentioned previously. Many of these attacks were instigated out of shared anti-U.S. objectives, whereas others were in exchange for the support Iraq provided the terrorist groups. In many cases there were previous linkages, and due to the expectation that Iraq would attempt to use the terrorism weapon, security and counter-terrorism forces were alert to these proxy activities.

While proxies generally share some goals or ideological basis with their sponsors or clients, this need not be the case. Purely mercenary proxy operations are possible, and sometimes even ideological opposites can find points where they can cooperate. The American Neo-Nazi and Christian Identity movements would seem to have nothing in common with Islamic fundamentalist groups, but in fact they have been cautiously exploring their shared anti-Semitism. Under the right conditions, this may prove to be enough agreement to lead to a proxy relationship.

For U.S. military forces, the most significant threat from a proxy attack is similar to the Gulf War scenario discussed above. A local or regional terrorist group could accept incentives to strike U.S. staging areas inaccessible to a hostile power against which the U.S. is deploying. Unlike Desert Storm, it is likely that some of these terrorist operations in the future will take place against units and facilities within the U.S. itself.

---

[144] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 52.
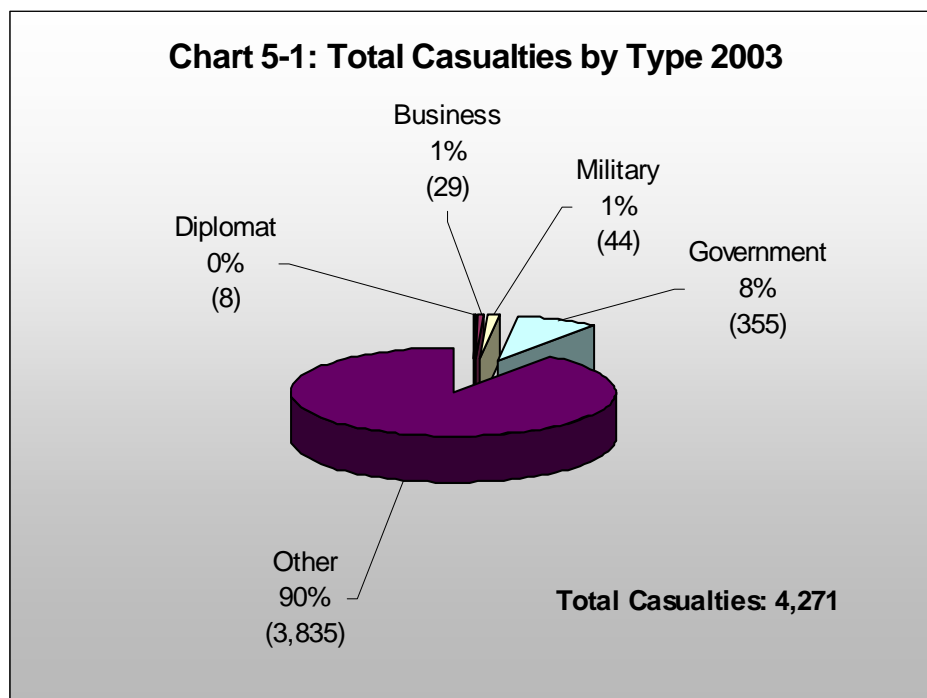
Conclusion

In this chapter we placed the threat to U.S. forces in a conceptual framework that allows unit planners and leaders to organize and interpret the threat information available to them. We have shown some of the motivations and objectives that exist for attacking military targets, and introduced a method of categorizing terrorist organizations in a militarily useful manner. In Chapter 5 we will look at the various categories of U.S. military forces in relation to terrorist threats.

Chapter 5
Terrorist Targeting of U.S. Military Forces

This chapter examines the threats to U.S. military forces. The intention is to provide a survey of likely terrorist actions. The descriptions are neither a region specific intelligence product nor an exhaustive list of terrorist scenarios, but does present techniques that have been used against U.S. forces in particular situations. Assessment and insight may assist risk management and situational awareness of potential terrorist activities.

Reviewing the casualties resulting from terrorist operations in 2003, there was an increase of nearly 140% in total casualties from 2002. Of the 4,271 casualties in 2003, the military accounted for 1% of the worldwide figures. Although this is relatively small compared to the large number of casualties in the "other" category (primarily civilians), Chart 5-1 demonstrates that government targets, which include the military, are definite objectives of terrorist attacks. Further, despite only three attacks directed at military facilities, versus 15 at diplomatic targets, military casualties exceeded diplomatic casualties by over five-to-one.[145] This indicates a significantly higher casualty rate per attack for military targets.

Chart 5-1: Total Casualties by Type 2003

Business 1% (29)

Military 1% (44)

Diplomat 0% (8)

Government 8% (355)

Other 90% (3,835)

Total Casualties: 4,271

Section I: Categories of U.S. Forces

In discussing the likelihood of particular threats to U.S. forces, situations are grouped in a simple classification of a military unit as deployed, deployable or in transit to

---

[145] Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2003* (Washington, D.C., April 2004, revised 22 June 2004), 5.

deploy/redeploy, or an organization that is nondeployable and operates permanently from a fixed location such as an installation or base. This system was used since terrorist targeting of U.S. vulnerabilities may be more concerned with the situational context of the unit at a particular place and time than with the unit's mission. Sections II through IV discuss each situation in detail.

Deployed Forces

This category consists of units that are deployed to locations other than their permanent base. Units that are normally stationed in Germany or Korea do not fit in this category. Because they are located overseas in those countries, U.S. forces have the infrastructure and local familiarity similar to a unit located at a continental U.S. (CONUS) post, base, or installation.

Deployed units are assumed to be operating away from their permanent bases, on either operational missions or training exercises. This category includes named contingency operations, fixed rotations into stability operations, and training assistance to foreign militaries, but is not intended to address individual assignments to overseas locations such as attaches or foreign study students.

Deployable/In Transit Forces

These units are either preparing for or in the process of deployment and redeployment operations. This includes active component units within CONUS or permanently based overseas, even if not currently identified for movement, and reserve component units that are identified for named operations or notified for mobilization.

Non-Deployable Forces

These are active and reserve component garrisons, training and logistic facilities, and other activities and installations that do not deploy to accomplish their organizational mission.

Section II: Terrorist Threat to Deployed Forces

In this chapter, risk to deployed forces is identified as primary, potential, and possible threats. These threats are expressed in general terms without actual terrorist group names, but include likely tactics, techniques, and procedures used against U.S. forces. Within this concept, terrorists understand normal measures of U.S forces operational security and force protection.

Environments and Conditions

Terrorists prefer to function in environments that reinforce their strengths and negate enemy advantages. They want to maintain secrecy while discovering enemy information, and focus on their objective while denying their adversary a concentration to strike and achieve surprise. In some cases urban terrain favors the terrorist in accomplishing these ends. Cities provide the terrorist with a population to conceal personnel, structures and facilities to hide and store equipment or weapons, and transportation nodes for movement. One example of terrorism in an urban environment is the Algerian quest for sovereignty in a violent period of post-World War II nationalism. (See text box below)

Regardless of the locale, terrorists will try to choose environments that are familiar to the terrorist but unfamiliar to U.S. forces. Additionally, terrain and locations that restrict the full use of military capabilities can be used to terrorist advantage.

Terrorists prefer an environment that is chaotic. A fluid, poorly policed or un-controlled situation often permits suspic-ious activities to go unnoticed. As a norm, terrorists prefer that the environment is not completely or continuously hostile. Hostile environments place military forces on their guard, reduce the opportunities to get close to targets without being chal-lenged or detained, and increase diffi-culty of achieving any degree of surprise.

Terrorist groups will normally avoid oper-ating as terrorists within actual combat-like environments. Doing so negates advantages and allows significant military strength to be used against terrorist oper-ations. These capabil-ities include battlefield intelligence and detection systems, weapons firepower, and reduced legal constraints on the use of force and the authority to arrest and detain, such as martial law or some variation of control.

The Impact of Martial Law – The Battle of Algiers

In the post-WWII surge of nationalist insurrections, the most notorious use of military authority to combat terrorism was the campaign waged by the French 10th Colonial Parachute Division against the urban terrorists of the Algerian insurgent movement FLN in the capital city of Algiers.

Algeria was one of the French colonies expecting to gain increased local rule, or perhaps independence, in the aftermath of WWII. When this did not occur, a nationalist insurgency began. By 1957 the nationalist groups, particularly the FLN, had been successfully carrying out a campaign of intimidation and terror that they felt would drive the French out of Algeria. The French responded by allowing the Army, in the person of General Massu and his *paras* [soldiers], to employ legalized barbarity against the FLN and suspected sympathizers. This included torture, mutilation, and murder.

The resulting campaign of terror and counter-terror has become known as the "Battle of Algiers," as much of the activity was initially concentrated in the capital city. While the French military scored significant successes, and broke the terrorist and guerilla forces in battle, they lost the war. Political support for the brutal suppression of the Algerians was eventually lost which directly contributed to the fall of the French constitution. After two attempted coups by French colonists in Algeria fearing that the mother country [France] was giving in, France finally granted Algerian independence in 1962.

However, terrorist operations can be successful during close combat operations. Chechen terrorists and paramilitary forces added psychological stress to Russian conventional operations in 1994-1995 during the attacks in the Grozny region. Separating terrorist activities from military action was difficult as tanker trucks were booby-trapped with explosives, roads were mined, and civilians were held hostage. Chechens were sent to misinform Russian forces about Chechen tactical plans, while some Chechens acted as a

network of informers on Russian movements. Reports spoke of Chechen men and women swearing an oath to commit subversive and terrorist actions in far away Moscow.[146] Examples of terror and counter-terror among military, paramilitary, and civilian populations are not unique to the Chechen issue.

Terrorists may use the advantages of surprise and security by hiding within a population. Sometimes terrorists may forego specific terror activities and operate as guerillas in areas of active combat operations. They can also operate as part of an insurgency force in combat operations. In Operation Iraqi Freedom, al Qaeda or foreign terrorists associated with al Qaeda have been involved in insurgency operations in Iraq since the inception of the war.

Terrorists know that deployed military forces will usually operate in one of two general environments of base camps or tactical (field) locations. Base camps are characterized by fixed facilities, either constructed or requisitioned, to provide shelter, support, and defensive capabilities to the units operating from them. This may include fixed airfields and port facilities. Base camps of military forces provide a much more stable and predictable target for terrorist planning. Of note, terrorist attacks carried out on U.S. units in Beirut (1983) and Khobar Towers in Saudi Arabia (1996) were in fixed billeting areas attacked by "purpose built" vehicle-borne improvised explosive devices (VBIEDs).

Tactical environments are considered to be those where the unit operates with only organic support in the field and no fixed facilities other than what the unit can improvise or what structures happen to be on the terrain. Units in tactical conditions have experienced casualties from gunfire and explosives but nothing comparable to the damage to the fixed facilities and related deaths of military members and civilians.

Terrorist incidents such as the sea-surface bombing of the USS *Cole* (2000) in Yemen illustrate the innovation of tactics and techniques against naval forces. Although Aden Harbor was not a permanent facility, the USS *Cole* was moored to a fixed refueling facility while in transit to its operational mission area. The Navy had been using the harbor for over a year for refueling operations. Terrorists had been conducting surveillance of these types of refueling operations and knew how long the ship would probably be in a fixed position in order to conduct a bomb attack.

Although deployed U.S. forces will be located in areas that are conducive, at times, to terrorist operations, these same forces have some advantages that can mitigate the risks of being targeted for terrorist operations. Several significant aspects are as follow:

- They are typically in a significantly enhanced force protection posture. Higher levels of alertness, control of approaches and access routes, and implementation of defensive measures reduce the likelihood of terrorist success, increase the costs to an attacker, and mitigate damage from successful attacks.

- They conduct appropriate planning and training to defeat or control hostile action. While this preparation may not specifically address terrorism, it does increase the probability of

---

[146] Alan C. Lowe, "Todo o Nada: Montonerosa Versus the Army: Urban Terrorism in Argentina," ed. William G. Robertson and Lawrence A. Yates, in *Block by Block: The Challenges of Urban Operations* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2003), 176-177.

effective defense against attack, and reduces the casualties and damage if an attack should occur.

- Deployed units typically have increased access to intelligence assets and products. This information increases the effectiveness of the unit's own intelligence, counter-intelligence, and force protection efforts.

Primary Threats

The primary threats to deployed forces will normally come from existing in-theater terrorist groups. This will often be in response to the U.S. military presence, or an attempt to influence U.S. policies in a region. Terrorist groups may try to minimize their movement of personnel and equipment into the area of operations after the arrival of U.S. forces to avoid detection. Whenever possible they will attempt to pre-position operational assets.

Figure 5-1. **Khobar Towers Dhahran, 1996**
(*Source*: DOD Photo)

A most dangerous form of attack historically used against deployed U.S. forces is the large vehicle-borne improvised explosive device (VBIED). This tactic has been used primarily against units in a base camp environment. The setback and protection common to deployed unit perimeters requires a powerful weapon to produce the large number of casualties and blast effects the terrorists want to achieve. A means to deliver adequate explosive weight to offset or negate layered security measures is a vehicle. VBIEDs equaling thousands of pounds of explosive power can produce the blast wave and secondary missile effects needed to cross security distances and still cause significant damage. The Khobar Towers VBIED was estimated to be the explosive equivalent of 20,000 pounds of TNT.[147] Table E-2 in Appendix E has a DOD chart that details the various size explosive devices with their comparable evacuation distances to avoid casualties.

A report in April 2004 by Jordanian intelligence indicated they thwarted an al Qaeda plan to detonate a large bomb in Amman with chemical weapon effects. The attack was targeting the Jordanian intelligence headquarters, as well as the U.S. Embassy and Jordanian prime minister's office. The exact type of bomb device was not disclosed, however, on-site estimates stated that up to 80,000 people could have been killed by this attack. The evolution of tactics planned in this attack, including reinforcing automotive vehicle body frames to crash through walls, indicates that terrorists continue to improve techniques of VBIED attack on their target locations.

[147] Department of Defense, *Report on Personal Accountability for Force Protection at Khobar Towers*, by William S. Cohen, (Washington, D.C., July 31, 1997), 2.

While possible that a unit in a field environment would be attacked by a large VBIED, it is much less likely than attacking a fixed facility. Preparation and deployment of such a weapon requires time that would likely be wasted if the target unit moved or improved its positions. This does not rule out the use of smaller IED weapons with faster preparation cycles if they can be effectively delivered and detonated. Lapses in security procedures, insufficient distance of personnel and facilities from a security perimeter, or habitually assembling units (convoys, patrols, road marches, etc.) in unsecured locations outside perimeters will be observed by terrorists as they seek a key vulnerability in security.

Delivering either a large or small explosive device by means of a suicide asset may or may not increase the effectiveness of such a weapon. The attack on the U.S. Marine Corps barracks in Beirut illustrates a successfully executed technique against a fixed facility. The suicide driver breached the gate and delivered the VBIED directly to the target. In this case, the use of a suicide bomber increased the probability and eventual effectiveness of the attack.

Conversely, at the Khobar Towers complex in Saudi Arabia, the vehicle access point was not considered an acceptable risk for breaching with a VBIED. Therefore, terrorists selected a point on the perimeter closest to the target buildings and people that allowed easy positioning of the VBIED, and a quick escape for the terrorists before the bomb exploded.

Variations of suicide attacks have been used to defeat specific perimeter security positions. One suicide asset acts as a breaching element in the first assault of a point. A second suicide asset follows immediately through the breach as an assault team with supporting fire from overwatch positions. This suicide element detonates the bomb to destroy a key target concentration within the target area.[148]

The most common form of attack used against deployed forces is the light weapons ambush, involving grenades, small arms, light bombs, and rocket launchers.[149] Additionally, IEDs are being used more often in these type attacks. These attacks have successfully caused U.S. military casualties and gained recurring international media coverage. They are the easiest and quickest type of attack to plan and stage.

The light weapons type of attack described above may be deliberately launched from a group of civilians. Attacks by combatants in civilian clothes can merge into civilian crowds. Attack may come from the cover of civilian centers like mosques, schools, or hospitals as occurred repeatedly during Operation Iraqi Freedom (OIF). This provides concealment for terrorists, as well as complicating a reaction from U.S. forces, since engaging a combatant, when shielded by non-combatants, could result in civilian casualties. Terrorists exploit civilian casualties for publicity and propaganda value. If the U.S. forces attempt to apprehend or neutralize an attacker without inflicting collateral non-combatant casualties, the U.S. action may be ineffective and expose the force to other attackers concealed within the group anticipating the U.S. attempt to limit civilian casualties.

---

[148] Rohan Gunaratna, "Suicide Terrorism in Sri Lanka and India," in *Countering Suicide Terrorism* (Herzliya, Israel: Interdisciplinary Center Projects Publishing House, 2002), 107.
[149] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 160.

In assessing the terrorist threat to a deployed force in a particular area of operations, the effectiveness of poorly resourced local groups should not be underestimated. Capabilities in terrorist organizations can differ significantly in their effects. Combined with intent and resolve, terrorist acts can be a major influence on U.S. national level decisionmaking on reinforcement or removal of U.S. forces from areas, as demonstrated in Beirut (1983) and Somalia (1992). While Somalia was not the result of planned terrorist action, the exploitation of the casualties and psychological impact from the failed U.S. mission are classic terrorist media techniques. "Actors" from outside the immediate area of operations supported U.S. adversaries in both of these incidents. Further, Somalia demonstrated the prestige that can be associated with successfully challenging U.S. forces, and bring benefits to the groups involved through increased support and improved perception by the local populace. These positive results become incentives for further attacks.

Potential Threats

Less likely than attacks by the existing in-theater groups are attacks by organizations that cannot otherwise reach U.S. targets either in CONUS or in other overseas areas. These groups will take the opportunity to attack U.S. military forces exposed in a third country. This can happen even if the U.S. forces are not a direct threat to the terrorist group, or are not conducting activities that are "objectionable" to the terrorists. The terrorists' attraction to the opportunity target of U.S. forces in a country that is a "permissive environment" is obvious. Such a country could be one with poor border control, a weak or unstable government, and easy access to weapons or smuggling routes. An attack could be exploited for objectives unrelated to the actual U.S. military mission.

In these circumstances the target of the attack may be more symbolic such as striking at significant individuals occupying positions of power or influence. Targeting senior commanders, particularly while in transit to or from a deployed unit in a permissive or exposed environment has been a frequent objective of terrorists. Attempted assassinations of key unit personnel should be considered a distinct possibility, with any number of methods available to the terrorist.

An example of this sort of "target of opportunity" operation was the bombing of the USS *Cole* in Aden harbor in October of 2000.[150] The presence of the USS *Cole* was unwelcome to

Figure 5-2. **Suicide Bomb Damage to USS *Cole*.**
(*Source*: U.S. Navy)

---

[150] John McWethy et al., no title, *ABCNews.Com,* (18 October 2000); available from http://www.abcnews.go.com/sections/world/ DailyNews/cole001018b.html; Internet; accessed 9 January 2003.

extremists who conducted the attack, and the situation created an opportunity for terrorist attack. The USS *Cole* was no direct threat to terrorist organizations ashore, and the refueling operation conducted in Aden was specifically meant to be unobtrusive to local sensibilities. However, the vulnerability of the ship indicated a high probability of success against an obvious symbol of the United States. Although the terrorist intention was probably to sink the warship, the resulting casualties and images of the damaged warship accomplished publicity and a psychological message on an international and worldwide audience.

The USS *Cole* bombing in 2000 used another VBIED, the vehicle in this case being a boat. Deployed forces should not ignore the possibility of explosive devices or other attack methods being delivered by boat or air. Various groups employed ultralight aircraft, powered and unpowered hang gliders, small civilian aircraft, and remote control aircraft to deliver attack teams, explosives, or suicide bombers to particular targets.[151] A unit that successfully interdicts or controls all surface approaches should neglect neither the possibility of an aerial approach, nor assume that control of surface approaches is sufficient. The Tamil Tigers (LTTE) have used suicide and remote-controlled explosive motorboats against Sri Lankan government targets. In 2000, they used suicide stealth boats to destroy a Sri Lankan fast personnel carrier and damage another boat. Also in 2002, a Palestinian suicide boat, a fishing boat packed with explosives,[152] intending to sink an Israeli naval craft exploded prematurely causing insignificant damage.[153]

Several terrorist groups have successfully utilized divers in underwater infiltrations and attacks. In 1975, the *Montoneros* terrorists in Argentina severely damaged the Argentine Navy's first modern missile-carrying frigate, the *Santisima Trinidad*. Divers approached the frigate in a camouflaged boat, attached underwater demolition charges to the ship's hull as it berthed in a naval shipyard under guard. The damage caused by the explosion delayed the ship's operational deployment for at least one year. A corresponding psychological impact accented a loss of confidence by the public in national military affairs.[154] In recent years, Israel has encountered terrorist divers attempting to enter through the sea.[155] Indicators point to subsurface terrorist attack as a recurring threat. Abu Sayaff terrorists kidnapped a diving instructor and demanded diving lessons. Similarly, a group of men approached a diving school in Kuala Lumpur to learn about underwater maneuvers but were uninterested in learning the skill of decompression when resurfacing.[156]

---

[151] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 165.

[152] "Fishing boat explodes near Israeli vessel," CNN.com./WORLD (22 November 2002); available from http://www.cnn.com/2002/WORLD/meast/11/22/mideast/; Internet; accessed 21 January 2004.

[153] *"The asymmetric threat from maritime terrorism,"* [database on-line]; available from http://jfs.janes.com/public/jfs/additional_info.shtml; Internet; accessed 2 February 2004.

[154] Alan C. Lowe, "Todo o Nada: Montonerosa Versus the Army: Urban Terrorism in Argentina," ed. William G. Robertson and Lawrence A. Yates, in *Block by Block: The Challenges of Urban Operations* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2003), 395.

[155] *"CAMERA ALERT: CBS' 60 Minutes Exposes "The Arafat Papers,"* Committee for Accuracy in Middle East Reporting in America; available from http://www.camera.org/index.asp?x_article=289&x_context=3; Internet; accessed 2 February 2004.

[156] Shefali Rekhi, *"Next terror target,"* *Straits Times Interactive* (16 October 2003); available from http://www.google.com/search?hl=en&lr=&ie=UTF-8&q=terrro+AND+attack+AND+underwater&btnG=Google+Search; Internet; accessed 21 January 2004.

A potential threat that has been employed against other nations' military forces with some success is the capture or kidnap of small units or individuals on missions that isolate them from the larger unit. The individual soldiers may be used as hostages, tortured, or killed for psychological effect. U.S. prisoners of war found themselves used as human shields, hostages, and worse in previous conventional conflicts. However, a recent example of this type of threat is the kidnapping and alleged killing of an American soldier in Iraq in June 2004. Specialist Keith Maupin was captured during an ambush on a convoy in April 2004 and had been held hostage for nearly three months. The Arabic television station Al-Jazeera initially aired a video showing Maupin in captivity on April 16, 2004. In June 2004 Al-Jazeera reported that Maupin had been killed by his captors. The television station aired a video showing a blindfolded man, allegedly Specialist Maupin, sitting on the ground. Al-Jazeera said that in the next scene, gunmen shot the man in the back of the head, in front of a hole dug in the ground. The hostage-takers' statement claimed that Maupin had been executed "because the United States hasn't changed its policy on Iraq and to avenge our martyrs in Iraq, Algeria and Saudi Arabia," according to Al-Jazeera.

Individual U.S. government and military personnel have been kidnapped and exploited by terrorists when serving on individual missions overseas. In 1981, members of the Red Brigades abducted U.S. Army Brigadier General James Dozier in Verona, Italy. Terrorists entered the Dozier's apartment, tied up his wife, and departed with General Dozier.[157] Stuffing Dozier into a trunk, the terrorists drove away in a car and hid Dozier in a safehouse. Eventually, they released a photograph to the media of a bruised and battered Dozier. With significant U.S. intelligence and Italian anti-terrorist investigation, an elite Italian anti-terrorism police unit rescued Dozier in a surprise assault on the safehouse.[158]

The uses of "atrocity videos", such as showing the torture and murder of prisoners in the Balkan, Algerian, and Afghan (Soviet) conflicts, are becoming common practice among terrorist organizations to attract and indoctrinate recruits, and terrify the opposition.[159] In May and June 2004, the gruesome beheadings of two Americans and one Korean by terrorists and the display of the murder on the Internet is a clear indicator that this tactic will continue to be used to exploit captured personnel for terror effects.

Other Possible Threats

Other possible threats include provocations by external or internal politically affiliated terrorist groups to induce U.S. action to achieve a desired outcome. In the Balkans, for example, the various ethnic and religious factions continually attempt to blame each other for harassment, graffiti, arson, and drive-by shootings. In fact, some groups would carry out incidents against their own property and people, and attempt to implicate their opponents to

---

[157] *"Red Brigades Kidnap an American General in Verona," New York Times*, 18 December 1981.

[158] "Operation Winter Harvest: The Rescue of Brigadier James Dozier," *Special Operations. Com*; [database on-line]; available from http://www.specialoperations.com/Counterterrorism/Dozier.html; Internet; accessed 26 February 2004.

[159] Jason Burke, "You Have to Kill in the Name of Allah until You are Killed," *Guardian Unlimited* (Observer Special Report, 27 January 2002), 3; available from
http://www.observer.co.uk/islam/story/0,1442,640288,00.html; Internet; accessed 15 January 2003.

provide a suitable cause for SFOR (Stabilization Force) involvement.[160] Their goal was to provoke SFOR into suppressive action against their enemies.

Another potential threat is the possibility of punitive attacks against family members of forward deployed personnel. This could be either retaliation for actions taken by U.S. forces, or a preemptive action designed to lower morale and decrease unit effectiveness. It could also be intended to provoke reprisals by U.S. soldiers against civilians in the area of operations.

Such attacks would depend upon the operational reach of the terrorist adversary, or their ability to engage a proxy organization to conduct such an operation for them. If actual attacks are impractical, threatening messages directed at family members could be employed to erode soldier confidence and morale. Falsified emergency notifications and Red Cross messages could be employed to the same effect. In fact, during OIF there were a number of cases where families received false notification that their relatives had either been captured or killed. In one week in April 2003, callers posing as American Red Cross workers informed family members in California, Delaware, Michigan, and Alabama that their family member had been killed in Iraq.[161] Although these examples may not be terrorist inspired, the issue of harassment and threats, as well as physical violence, can further stress an environment already experiencing fear and anxiety.

Preventative Measures

The greatest deterrent to terrorist action is aggressive operations security (OPSEC) programs emphasizing surveillance detection and counter-intelligence activities. While physical security measures are essential, they can be neutralized or avoided by terrorists with adequate preparation. Terrorists must have superior target intelligence to select targets, circumvent security, and plan operations. Deny them this information, and they cannot operate effectively. Detecting them collecting target data permits anticipation of possible terrorist courses of action.

Information the deployed unit should consider obtaining includes any record of surveillance incidents directed against U.S. diplomatic or commercial activities in the country. Correlation of confirmed surveillance against these potential targets permits a deployed unit to identify personnel, vehicles and techniques in use in that area prior to arrival. Terrorists have the capability to use sophisticated tradecraft that will complicate this correlation, but they have also been known to use the same personnel and vehicle repeatedly in surveillance tasks. The Khobar Towers pre-attack surveillance was conducted using one vehicle for all surveillance missions. That vehicle was observed and reported 10 times out of 40 separate uses as a surveillance platform.[162] Unfortunately, this information was not correlated and interpreted correctly by U.S. forces.

---

[160] Department of Defense, *11th Psychological Operations Task Force After Action Report for SFOR X*, by MAJ Clint A. Venekamp, (Upper Marboro, MD, July 2002).

[161] "False Calls on Casualties Upset Camp Pendleton Spouses," *Mustang Daily Online News*, 11 April 2003; available from http://www.mustangdaily.calpoly.edu/archive/20030411/print.php?story=inat; Internet; accessed 13 August 2004.

[162] Department of State, Bureau of Diplomatic Security, *State Department Diplomatic Security Surveillance Detection Program Course of Instruction* [CD-ROM], (Washington, D.C., October 1999).

Unit planners should seek out any record of actual terrorist activities in the area, whether directed against U.S. interests or not, from intelligence, security and law enforcement sources. Additionally, groups or individuals considered dormant or inactive should be reviewed based upon the possible change in attitude or motivation that a U.S. deployment into the area might cause.

Variation of a unit's operational patterns is a basic but useful technique to deter attacks. It prevents anticipation of target actions by the terrorist(s); it introduces uncertainty to his planning, and sharpens the alertness and observations of unit personnel by avoiding routine. Terrorist operations have been called off, and attacks in progress have been "blown" due to simple changes in the routine or activity of a target.

This is by no means an exhaustive list of threats to deployed U.S. forces. Intelligence specific to the area of operations must be studied and integrated into realistic threat assessments for deployed units. However, terrorists have used the techniques mentioned in the scenarios discussed here multiple times against deployed military forces. These techniques will continue to be employed by terrorists in modified forms with innovations in weapons or tactics as long as they continue to be effective.

Section III: Terrorist Threat to Deployable Forces

This section discusses likely threats to U.S. forces in the deployable category. "Deployable forces" are those units that are either preparing for or in the process of deployment and redeployment overseas. These units include active component units both within CONUS and permanently based overseas, (even if not currently identified for movement) and reserve component units that are identified for named operations or notified for mobilization. The purpose for identifying "deployable" units in this manner allows us to consider possible threats to a unit ranging from their home station to their debarkation point during a deployment. Additionally, this category addresses those threats directed at war fighting or operational units not immediately slated for movement. Installations will be discussed in Section IV.

Reserve component units identified for mobilization or participation in named operations fall into this category even though their deployment may not be imminent. This is because of the increase in training activity and resources they receive, as well as the possibility that their participation in a particular operation will motivate an attack. When discussing home station activities, attacks planned against off-duty personnel known to be military members are also considered.

Primary Threats

Threats to deployable U.S. forces, either at home station or in transit to and from an operational mission, may be from foreign or domestic terrorists. Foreign terrorist organizations will be international or transnational groups with either an operational presence already in the U.S., or support infrastructure in place to facilitate the arrival of operational assets. They will possibly be state sponsored organizations, or organizations operating for profit or for other material considerations on behalf of some government. In some cases they could be state intelligence or covert military special operations forces. Domestic terrorist

groups may arise from any number of special interests with political, social, religious, or environmental focus. While in raw numbers of past incidents, domestic terror groups were responsible for more attacks and attempted attacks on U.S. military targets than external groups, most of these attacks were directed against facilities and installations, not units and personnel.

However, state sponsors or transnational terror groups may also use domestic groups that can be exploited through shared ideology or for monetary considerations to conduct operations in the U.S. against military targets. For instance, the El Rukns group, a Chicago based gang, negotiated with Libya to attack a domestic airliner with a surface to air missile in 1985.[163] Apparently, Libya postponed the attack when the group purchased a light anti-tank weapon from an undercover FBI agent. The group's leader and six other El Rukns were arrested and subsequently convicted of conspiracy to commit terrorism. Libya also directed and sponsored lethal attacks by the Japanese Red Army (JRA) on U.S. military targets in CONUS and abroad during the same period of time.[164] In CONUS, a JRA member was apprehended in 1998 with three pipe bombs in his car, the target supposedly being a U.S. military base. In this case, Libya could probably have used a domestic U.S. group had one been available and capable. Overseas, a 1998 JRA bombing of a U.S. servicemen's club in Naples, Italy killed five people including a U.S. servicewoman. Although these examples occurred in the 1980s, there is also evidence indicating that al Qaeda is subcontracting to like-minded terrorist groups to conduct operations.

Home Station Threats

Threats to deployable units at their home station during pre-deployment activities will most likely consist of attacks on units conducting movement to or from training activities, and attacks upon off duty personnel during social gatherings. The intent would be to demonstrate the capability to damage U.S. military forces, and weaken morale. The most likely methods of attack would be a small to medium size improvised explosive device (IED), or an ambush conducted with light weapons (automatic weapons, grenades, and anti-tank rockets).

Attacks on units training will most likely take place during movement because:

- The unit is concentrated during movement, and typically dispersed during training.

- Training areas are usually harder to access by non-military personnel than roads leading to or from them.

- Units training have a greater degree of alertness than units in an administrative road movement.

- Units conducting training have greater self-defense capabilities, especially if they are training with live ammunition.

---

[163] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 162.
[164] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998),   188-189. The JRA adopted the name "Anti-Imperialist International Brigades" for these operations.

- Routes to and from training areas are well established, almost habitual, whereas movement during training is more difficult to pattern.

Attacks on personnel at social gatherings can occur at clubs on post, or during unit functions at private homes or commercial establishments off post. Traditional observances of organizational days, town hall meetings, and family support briefings are often publicized in advance and give attackers planning dates for possible gatherings in accessible locations. Attacks at commercial entertainment establishments such as bars, clubs and restaurants off post are less likely because the density of military personnel at a particular establishment is usually not sufficient to gain the appropriate impact. The most likely attack method will be a small to medium sized IED, although terrorists may employ improvised mortars or other standoff weapons.

Deployment Preparation and Movement

Attacks on deployable units are likely to occur during actual preparation for deployment activities. The specific mission may inspire an attack by a group who wishes to prevent the deployment, or a potential adversary may attempt to extend the depth of the battlefield by engaging units with unconventional terrorist attacks before they arrive in theater. Objectives of these attacks will depend on the mission of the deploying unit and the context of the mobilization, but may include:

- To delay or prevent mobilization or deployment.

- To render the unit non-mission capable for deployment.

- To decrease unit effectiveness when deployed.

Delay or Prevent Mobilization or Deployment

Operations aimed at this objective would involve either disrupting the unit enough to prevent its movement on schedule, or disrupting the transportation cycle for the unit. Disruptions sufficient to prevent the unit from making movement would probably also render it non-mission capable for deployment.

Disruption of transportation may take place by sabotage or direct attack upon the unit being transported and its conveyance. Methods of attack would be selected depending upon their effectiveness versus the mode of unit transport. Air, rail and sea are the modes of transport for long voyages, but frequently units must use ground conveyances such as buses or organic vehicles to get to their embarkation point. Consequently, attacks may also occur against these vehicular movements. Weapons likely to be employed include bombs, AT rockets, and potentially, guided missiles. If sabotage is used in preference to direct attack, the sabotage will be designed to produce maximum casualties in the ensuing crash, derailment, fire, etc. An example of this type threat was demonstrated in January 2003 when intelligence sources detected the targeting of chartered aircraft participating in the build up of forces against

Iraq.[165] Additionally, domestic terrorists have derailed U.S. passenger and cargo trains,[166] and attacks on ships in port and at sea are well within the capabilities of most transnational and international terror groups.

Destroying facilities such as docks, airfields, refueling facilities, and cargo terminals at intermediate stops or at the final destination is another way for terrorists to prevent or delay deployment. Attacking critical private infrastructure, both through physical and cyber means, could cause similar effects. It is a method of adding depth to the battlefield during a conflict, and does not require the projection of assets and weapons into more distant countries. If timed to coincide with the arrival of incoming units, such destructive attacks could cause significant casualties. The *Montoneras* terrorists, having advanced from individual terrorist acts to paramilitary guerrilla operations, achieved significant psychological strikes to Argentine military forces using this type of attack against an air force airfield in 1975 with spectacular results. Placing explosives in an abandoned tunnel underneath the airfield runway, the bomb was detonated as a C-130 aircraft carrying an antiguerrilla unit was starting its departure. The C-130 was destroyed, resulting in four killed and forty injured, as well as damaging the runway. At a minimum, this was a psychological blow to the Army's image with its nation, and a clear instance of a military force defeat.[167]

Render the Unit Non-mission Capable for Deployment

The objective here is to cause sufficient damage or disruption to the unit so that it will be unable to deploy, or will be unable to function once deployed. The most direct way to do this is to inflict casualties on the unit. IEDs, rocket launchers, and mortars directed at unit assemblies such as formations, manifest calls, and other pre-deployment personnel concentrations are the most likely scenario. A terrorist group with a rudimentary biological weapons capability could infect enough of a unit with a contagious disease that it would have to undergo quarantine, delaying deployment. Additionally, terrorist capability and suspected or known intention to use biological weapons against U.S. military forces could cause extraordinary processes for vaccination of U.S. military forces. These additional preventive medicine and safety issues may result in longer deployment timeframes for U.S. military forces. The use of biological weapons is a less likely and somewhat uncertain proposal from the terrorist point of view, but could be used to bypass defenses designed to prevent other forms of attack. Additionally, given al Qaeda's statement that it is their "holy duty" to acquire weapons of mass destruction, it is clearly an option that terrorists are pursuing.

Another possibility to consider is the destruction of a key piece of equipment or the assassination of key personnel. This is less attractive to the terrorists because they cannot be sure that such losses would not be rapidly replaced. Unless the terrorist group is aware of specific personnel or equipment shortages, they will rely on the more certain method of mass casualties.

---

[165] Thom Shanker, "Officials Reveal Threat to Troops Deploying to Gulf," *New York Times,* 13 January 2003; available from http://www.nytimes.com/2003/01/13/politics/13INTE.html; Internet; accessed 13 January 2003.
[166] Jim Hill, "Sabotage Suspected in 'Terrorist' Derailment," *CNN.com*, 10 October 1995; available from http://www.cnn.com/US/9510/amtrak/10-10/; Internet; accessed 15 January 2003.
[167] Alan C. Lowe, "Todo o Nada: Montonerosa Versus the Army: Urban Terrorism in Argentina," ed. William G. Robertson and Lawrence A. Yates, in *Block by Block: The Challenges of Urban Operations* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2003), 395.

Decrease Unit Effectiveness When Deployed

This objective requires actions to undermine morale and destroy unit efficiency. It will be characterized by less lethal, more harassing activities. Contaminating unit equipment with low level radiation sources, infecting unit information processing equipment with viruses, harassing or attacking soldiers' family members, and inserting false messages of death or illness into the various notification systems to both family and service members are all possible scenarios. With the exception of actual attacks on service members' families, these activities do not require significant operational skill or resources.

Potential Threats

Home Station Vulnerabilities

Although less likely than transnational or international terrorists attacks, domestic groups who object to U.S. military involvement overseas, or to the political goals of U.S. policy still have potential to conduct attacks. Such groups would share the objectives listed above, with the further aim of publicizing the domestic dissent to the particular mission or policy. Such groups could develop capabilities very rapidly, and commit acts that disrupt, damage, or delay institutional support to military forces. Although they are nearer to the targets and less visible to casual suspicions than foreign personnel, domestic terrorists would be constrained in conducting significant lethal attacks due to the possibility of severe backlash for actions against fellow citizens.[168] Actions would probably start out with symbolic and non-lethal arson, vandalism, and sabotage. If these fail to ignite public support for the terrorists' goals, their organizations would increase in radicalization, and attacks would become more lethal, as happened in the Vietnam-era anti-war movement.[169] In 2003, a militant spokesperson openly recommended that like-minded supporters "…Actively target U.S. military establishments within the United States." Stated goals are to "…disrupt the war machine, the U.S. economy, and the overall functioning of U.S. society…"[170]

There is also the potential for domestic groups to attempt to obtain advanced military technology or new equipment by raiding units during normal training activities. This threat is most likely to come from groups who wish to rapidly increase their offensive capabilities in anticipation of paramilitary operations. Groups whose ideology emphasizes insurrection, social warfare, or "local" uprisings are most likely to attempt this type action. There are many examples of this threat in the United States. In the mid-1990s, a militia member in Florida was charged with planning to break into a National Guard armory to steal explosives and firearms. These capabilities were to assist his intention of blowing up power transmission lines that feed a large city and nuclear plant. The indictment also stated that the individual plotted to kill a militia member suspected to be an informant. Federal authorities

---

[168] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 94.

[169] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Student Terror: The Weathermen."

[170] Craig Rosenbraugh, "Craig Rosenbraugh on the Anti-War Struggle," *Houston Independent Media Center*, 17 March 2003; available from http://houston.indymedia.org/news/2003/03/9125.php ; Internet; accessed 16 February 2004.

seized rifles, handguns, and a large quantity of ammunition from the individual's home.[171] Also in the mid 1990s, members of the Michigan Militia were apprehended with a car containing 700 rounds of ammunition, loaded rifles, night vision goggles, and other military-type equipment.[172] In 2001, a white supremacist was charged with stockpiling bomb making materials and bank robbing. This individual also attempted to use counterfeit paper currency. A notebook at his lodging included recipes for bombs mixing fuel oil and fertilizer similar to the bomb used in the Oklahoma City bombing of the Murrah Federal Building.[173]

This domestic threat is not just limited to small explosives and firearms. In 2003, a Texas citizen pleaded guilty to possession of a weapon of mass destruction. In a Federal investigation that started due to finding false government identification badges, subsequent searches at the individual's home and storage facility uncovered a sodium-cyanide bomb capable of killing thousands, a large amount of explosives, 500,000 rounds of ammunition, dozens of illegal weapons, and a large number of white supremacist and anti-government literature.[174]

Deployment Preparation and Movement

As discussed above, domestic groups who object to U.S. military activity or U.S. policy could conduct operations against deploying units. A key difference here is that attacks of this nature would probably start out at the lethal end of the spectrum. This is because the domestic groups are either conducting operations sponsored or directed by external actors, such as other terrorist groups or nations, or because imminent deployment would increase the sense of radicalization of these groups. Such groups would share the objectives for preventing or delaying unit movements discussed under "Probable Threats," with the further aim of using such actions to publicize their dissent.

A particular specialty of domestic groups is their capability to conduct harassment campaigns against individuals peripherally associated with or employed by activities these groups object to. Such a campaign undertaken by a domestic group against service members' families with the objective to reduce unit morale and effectiveness would be extremely disruptive. Harassment campaigns have included lethal and near lethal attacks, as well as disrupting the victim's daily life and instilling constant, pervasive fear in the victim. Such a campaign added to the normal stresses associated to military careers and deployments could have extremely negative consequences in both the long and short term.

---

[171] Larry Dougherty, "Indictment details plot to blow up power lines," *St. Petersburg Times*, 9 December 1999; available from http://www.sptimes.com/News/120999/TampaBay/Indictment_details_pl.shtml; Internet; accessed 16 February 2004.

[172] Tom Burghardt, "Leaderless Resistance and the Oklahoma City Bombing," BACORR: Bay Area Coalition for Our Reproductive Rights; available from http://nwcitizen.com/publicgood/reports/leadless.htm; Internet; accessed 10 February 2004.

[173] Shelley Murphy, "White Supremacist Accused of Targeting D.C. Museum," Globe, 20 September 2001; available from http://www.rickross.com/reference/supremacists/supremacists57.html; Internet; accessed 16 February 2004.

[174] Kris Axtman, "The Terror Threat At Home, Often Overlooked," *Christian Science Monitor*; 29 December 2003; available at http://ebird.afis.osd.mil/ebfiles/s20031229244982.html; Internet; accessed 29 December 2003.

Possible Threats

Possible threats to both home station activities and deployment activities could come from U.S. resident aliens or citizens not specifically organized or affiliated with larger terrorist networks. These groups may have loyalties to ethnic, religious, or nationalist causes hostile to the U.S. or opposed to U.S. policies. Expatriate and immigrant ethnic groups threatened action against government and military targets in the U.S. and Europe when Stabilization Force (SFOR) activities or policies in Bosnia-Herzegovina were perceived as contrary to the best interest of their ethnic "home" state or group. Other immigrant and expatriate groups have provided support for various hostile activities directed against particular U.S. foreign policies. While largely unorganized, even individuals with little support but high motivation can have major impacts. Jordanian Sirhan Bishara Sirhan assassinated Senator Robert Kennedy in 1968 because of his assumption that Kennedy would likely be the next U.S. President, and he wished to prevent Kennedy's expected support for Israel. Probably the best-known example of an individual domestic terrorist incident, though, is Timothy McVeigh's bombing of the Murrah Federal Building in Oklahoma City. His hatred of the Federal Government and his belief that U.S. Government policies and practices were unjust and violated citizens' Constitutional rights drove him to conduct this heinous act.

Units Based Overseas

Units based in overseas locations have several special considerations. Because of different conditions outside of continental U.S. locations, their home station routine is more vulnerable to terrorist attack than similar units based inside the continental U.S. Europe is an excellent example where attacks on U.S. service members have been extensive and lethal.[175] Some attacks were state sponsored or directed, which made them even more dangerous.[176]

There are two principal conditions contributing to the higher level of threat to overseas-based units. The first condition is exposure. Countries that have permissive border controls, countries that are located closer to states that harbor or sponsor terrorists, or that have active terrorist groups within their borders, all increase the ability of terrorists to reach U.S. military units and personnel based therein. This situation is best illustrated in Europe, where internal border control between European Union (EU) nations is no longer required. Once the borders of a EU member are penetrated, travel to all member countries becomes possible with minimal control. The proximity of the EU to states sponsoring terrorism is much greater than the U.S., and the smuggling and criminal trafficking routes used by terror groups pass through or close by EU nations. Additionally, several EU nations still have very capable terrorist organizations based within their borders.

Conditions may be posed by the host nation (HN) that constrains U.S. military forces from implementing force protection measures such as stand-off distance, barricades, and patrols outside a facility perimeter. U.S. military forces at Khobar Towers (1996) witnessed such constraints. Also, criminal organizations loosely or closely linked to terrorist groups, can cause dispersal of limited resources and capabilities such as U.S. military police, contracted security forces, or other anti- and counter-terrorism assets.

---

[175] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Chronology of Terrorist Events."
[176] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 71.

The second condition is visibility. U.S. military members are usually highly visible in overseas environments, particularly in countries that emphasize their homogeneity. This not only aids in targeting U.S. personnel; but also contributes to another kind of visibility - political visibility. U.S. military presence is frequently a contentious issue in local politics in host nations. This political visibility can lead to resentment of the U.S. presence, and ultimately to attacks against visible signs of that presence, such as military personnel. It is often difficult, though, to determine if a terrorist element or just political activists within the country instigate these attacks. Excellent examples are the common protests in South Korea against the presence of American troops in the country. One occurrence happened in November 2002, when South Korean activists hurled firebombs into a US military base in protest against the acquittal of two American soldiers who ran over and killed two South Korean girls. During the protests, American troops were kicked and beaten by the protesters before they could be contained.

The most common threat to overseas-based units is attacks directed against off-duty personnel, either at social gatherings or at entertainment establishments. This is different from the home station situation for CONUS based units because personnel overseas tend to cluster socially, frequenting particular establishments in large numbers. This density provides sufficient military victims for the terrorist attack to achieve the desired effect. Also, significant civilian casualties can be exploited as a wedge issue, to be driven between the host nation populace and the U.S. military. To the terrorists, causing civilian casualties at a club in an American town would simply be more dead Americans. Attempting to instill negative feelings toward the military in the local community would be nearly impossible. However, dead civilians from a host nation can be "blamed" on the U.S. presence by the terrorists, and can raise the question in the host nation political system of the costs of hosting foreigners who are going to attract political violence to their communities. This specific threat was demonstrated in April 1988 when a car bomb exploded in front of the USO Club in Naples, Italy. The explosion resulted in the death of five people, including a U.S. servicewoman. Additionally, fifteen people were injured, including four U.S. servicemen. Junzo Okudaira, a Japanese Red Army (JRA) member, was indicted for the bombing.

Other attacks that have been conducted against units based overseas have principally involved rocket launchers, improvised mortars, and bombs directed against key leaders and on-duty personnel. These attacks have ranged from the low end of sophistication to highly technical operations. While unlikely, the possible use of chemical or biological weapons should be acknowledged. The 1995 Tokyo subway nerve agent attack was conducted by the Aum Shinrikyo cult, which was (and is) virulently anti-American. Aum Shinrikyo had a significant interest in all forms of WMDs, and in addition to the nerve agent Sarin, had several other types of chemical and biological weapons under development.[177] Aum's central philosophy focused on the inevitability of nuclear Armageddon, and the cult occasionally considered provoking such a conflict so they could fulfill their appointed role in such a disaster.

Vandalism, sabotage and arson attacks have also been used for symbolic effects, but are usually intended to be non-lethal. These types of actions can occur during political

---

[177] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 125.

demonstrations against U.S. military presence as a provocation to host government police or U.S. security personnel to further polarize attitudes.

Protection Measures

Denying terrorists the target information they require is the most certain deterrent. Unlike deployed units, deployable units will have installation security measures, functioning local law enforcement activities, and other non-military security and investigation organizations operating in their environment. Therefore the unit operational security (OPSEC), force protection, and security programs are not the only reliable resources available to the unit planner.

Access control is one aspect of unit training that can assist in denying the terrorist target information. Because units are stationed within functioning communities, there are many interactions with non-military individuals and activities. Since there are multiple jurisdictions involved, there are various legitimate permissions to access military posts. Unit personnel should be familiar with the various types of access control documents they will encounter. If required to establish or man access control points, unit leaders should become familiar with the capabilities of common counterfeiting technologies and their effectiveness in duplicating access control and identification documents. Due to advances in digital camera and image enhancement technology, loss or theft of documents is no longer necessary for reproduction. Likewise, electro-optical zoom lenses and hidden micro-cameras can gather keypad combinations and PIN numbers for security systems.[178] Unit planners need to understand these new vulnerabilities in order to mitigate them where possible.

Deployable forces face a variety of threats, but most are relative to their role as war fighting organizations either preparing for or moving to their missions. Their value as a terrorist target is driven by policy decisions beyond their ability to affect and may be subject to attempts to expand potential conflicts to the U.S. homeland. Therefore anticipation and alertness are the most important factors in mitigating the threat.

Section IV: Terrorist Threat to Non-Deployable Forces

This section focuses on threats as applied to U.S. forces in the non-deployable category. Non-deployable forces consist of installations, fixed infrastructure, and training establishments. It also includes National Guard and Reserve units and facilities not currently listed for deployment. Since these activities are more or less permanently fixed, discussion considers the likely threats for the United States and its' territories. Also, since these activities provide the logistic and power projection capabilities for any deployment of U.S. forces, they are likely targets of terrorist groups.

Threats discussed in this section survey attack likelihood, covering primary, potential, and possible threats. While deployable and deployed forces are particularly at risk during conflict or times of international tension, non-deployable forces will experience threats based upon

---

[178] Paul Kaihla, "Forging Terror," *Business 2.0* (December 2002): 3; available from http://www.business2.com/articles/mag/0,1640,45486%7C5,00.html; Internet; accessed 22 November 2002.

domestic political tensions as well. These tensions could inspire action by a variety of social and single-issue domestic extremists from all sides of the political spectrum.

Primary Threats

The most probable threats to non-deployable forces of all kinds will likely be domestic groups with a variety of objectives. While the domestic terrorism landscape is cluttered with any number of ideological and religious motivations, most U.S. domestic terror groups have embraced the "leaderless resistance" model of organization. While this tends to limit the complexity and sophistication of these operations, it also reduces the effectiveness of infiltrating the group or developing informers, because of the decentralized nature of operations (See below).[179] As the Oklahoma City bombing conclusively showed, "simple" attacks do not necessarily equal "ineffective" or "non-lethal" attacks.

Leaderless Resistance

Simply put, leaderless resistance involves individuals or extremely small groups (two or three persons) who share common goals and values with a larger whole. They remain unaware of each other, and rely upon themselves to conduct actions against the enemy. While it bears similarities to network style organizations, the lack of communications links between nodes makes it more like a mob or riot phenomenon. Everyone in it seems to know what to do collectively, with little communication.

There is usually an ideological center to such groups; an individual or cabal who sets the tone for the larger mass. This center remains unaware of the radical members and their intentions. They outline an ideal condition or future to be achieved, and then exhort their followers to obtain it, without going into specifics on the method to be employed. "You know what to do" is the mission order in this environment, allowing the "leader" to avoid incitement or conspiracy charges, while claiming credit for the work of the unknown individuals or cells.

One of the major threats in this category is an attack against U.S. military forces and installations to obtain weapons or equipment. In the 1970s alone, enough small arms were stolen from U.S. military facilities to outfit a force of approximately 8,000.[180] These operations are conducted by a variety of groups, but most recently groups associated with white supremacists, various "Christian Identity" offshoots, or the "militia" movement predominate in this area. They are conducted as "inside jobs" or theft more often than actual overt raids or attacks, but the capability and inclination for violent operations is there. If the terrorist group believes the objective warrants it, assault style robberies of military equipment will occur.

---

[179] Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999,* Report 0308, (Washington, D.C., n.d.), 18.

[180] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 111.

Another likely threat is that transnational or state sponsored groups could target key infrastructure or support installations to reduce the military's power projection capabilities. In fact, these type targets are on al Qaeda's targeting list. In July 2001, Ahmed Ressam, who was trained at al Qaeda camps in Afghanistan, testified that he had been trained to blow up various types of targets, to include military installations, airports, railroads, electric plants, and gas plants. Additionally, there are reports of al Qaeda surveillance of critical infrastructure targets and an FBI Information Bulletin states that al Qaeda members have sought information on Supervisory Control and Data Acquisition (SCADA) systems, which are computer-controlled devices used to monitor and control much of our critical infrastructure.[181] These SCADA systems are potential targets of cyber-terrorism. (See Cyber Operations appendix for more information on cyber-terrorism.)

Although a major attack has not occurred against U.S. critical infrastructure yet, al Qaeda has a presence in the United States. This transnational presence was exhibited in 2002 when two suspected al Qaeda cells were neutralized; one in Portland, Oregon and another in Lackawanna, New York. Well-funded adversaries without a significant operational presence in the U.S., or who desire deniability, could instigate attacks utilizing various domestic groups as proxies. Money or common ideology or goals would provide the basis for this cooperation. This sort of attack would have slightly different objectives than those discussed in Section III. The destruction of critical logistics and transportation infrastructure such as rail lines, pipelines, and warehouses would emphasize arson and sabotage. Unfortunately, these capabilities are highly developed in most of the domestic U.S. groups that could act as proxies for a hostile foreign entity.

In looking at threats that involve facilities and infrastructure, consideration must also be given to attacks on information systems and computer networks. Attacks directed against military systems, and designed to damage, not annoy, took place during the NATO air campaign against Serbia in 1999. Physical destruction of unprotected network components, or increasingly available technology that interrupts or damages computer circuitry from a distance may emerge as the most dangerous of these threats,[182] although malicious hacking and viruses will continue to be the most common. See Cyber Operations appendix for more information on cyber-terrorism.

Another type of target that might be selected for the sheer psychological impact is the highly symbolic target. The attack on the Pentagon in 2001 is an outstanding example of an attack with this objective. Many other posts have less famous, but still symbolically significant monuments and activities that could be subject to attacks under this scenario. In April 2004, Department of Homeland Security Secretary Tom Ridge voiced his concerns over the potential targeting of symbolic events that could be targeted by terrorists, including the dedication of the World War II memorial, Fourth of July celebrations (which often include military contingents), and the Democratic and Republican national conventions.[183]

---

[181] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 115.

[182] Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999,* Report 0308, (Washington, D.C., n.d.), 40.

[183] Adam Goldman, "Ridge Announces New Security Measures," *MyrtleBeachOnline.com*, 19 April 2004; available from

Military installations with a high concentration of military personnel and families could be attacked with some form of mass casualty weapon for the pure terror and psychological impact on the military services as a whole. Although the personal devastation this could cause would be serious enough, the resources required to counter future attacks could significantly degrade war-fighting capabilities.

Potential Threats

Domestic Threat To National Guard Armories
From "Terrorism in the United States, 1999" FBI Publication #0308

On December 8, 1999, Donald Beauregard, Commander and Brigadier General of the Southeastern States Alliance (SSA) was arrested on six felony counts related to his plans to steal weapons and explosives from National Guard armories in central Florida, attack power lines in several states, and ambush Federal law enforcement officers. The SSA was an "umbrella" organization composed of individuals from several militias in Florida, Georgia, South Carolina, Alabama, and other southern states. The objective of the now-defunct organization was to create social and political chaos, which members believed would cause the U.S. Government to declare martial law, thus inciting a popular uprising and violent overthrow of the Federal Government. The SSA theorized that Beauregard's plan would create this chaos and further their goal of violent revolution. Beauregard was charged with violating several Federal laws, including Title 18 USC Section 371, conspiracy to break into a military facility to steal weapons and explosives; Title 18 USC Section 2339, providing materials in support of a terrorist organization; and four counts relating to Title 26 USC, firearms violations–transferring a sawed-off shotgun, possession of a silencer, transfer of a firearm without a serial number, and manufacture of a sawed-off shotgun.

Conflicts over domestic social policies have a probability of causing attacks on military installations. While not participants in these policy debates, the U.S. military services have been the instruments of major social reform at the direction of both Congress and the Executive Branch. The military services have led the nation in implementation of social policies such as complete integration of racial minorities and women. Groups on both sides of contentious social issues in U.S. domestic politics watch various proposals regarding military implementation of policies regarding their particular causes. Decisions by Congress for or against military implementation of social policies on contentious domestic issues could very likely spark violence by the more radical elements of either side in these debates. The capabilities of groups involved in these issues, and the level of violence already displayed against other segments of society involved in a variety of contentious social issues make this a significant concern.

The emergence of a radicalized, ostensibly "anti-war" movement is also a distinct possibility. This sort of "anti-war" movement does not need an actual conflict to be initiated. "Anti-war" rhetoric and agendas have been incorporated into large protest gatherings such as "The Battle of Seattle" (Seattle World Trade Organization meetings in 1999) prior to the terror attacks on the U.S. and the subsequent military retaliation. The recent shifting and redefining of the

---

http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/special_packages/riskyrx/8466467.htm;
Internet; accessed 29 April 2004.

traditional "radical left" ideological focus to an anti-capitalist, anti-globalization, and "economic and social justice" agenda has made <u>any</u> military action by U.S. forces – whether the mission is humanitarian, disaster relief, or actual combat – suspect in their eyes. Many of the left wing and single-issue organizations that espouse the anti-capitalist, anti-globalization, and anti-war rhetoric are branches or offshoots of international organizations.[184] These groups maintain ideological linkages and copy operational techniques from foreign groups. The fact that the pace of military deployments on all missions has increased, and especially with ongoing operations in Afghanistan and Iraq, is seen by many of these groups as "proof" of U.S. "imperialism." These issues invite the targeting of U.S. military forces as the symbols and effective arms of these "imperial" policies or intended U.S. "hegemony."

There is also the possibility of attacks directed against military installations or personnel from single-issue terrorists focused on animal rights or environmental issues. The FBI considers these groups the largest domestic terror threat in the United States.[185] Although these groups typically conduct arson, harassment, and vandalism, they have gradually increased their capabilities and rhetoric, threatening to "pick up the gun" and to target Federal offices and Federal and state law enforcement.[186] It is expected that attacks are possible on range or post construction projects that they perceive as endangering animals, animal habitat, or the earth.

To highlight this potential threat, following a "Revolutionary Environmentalism" conference held at California State University at Fresno in 2003, Craig Rosebraugh the past spokesman for Earth Liberation Front (ELF) issued a manifesto calling for anti-war protesters to carry out direct actions against the U.S. Government and military installations. Specifically, he called for activists to "Actively target U.S. military establishments within the United States. Again, following the above stated goal of NOT getting caught, use any means necessary to slow down the functioning of the murdering body." [187]

Military research using animals for testing chemical or biological weapon antidotes or medical treatments could also spark direct action and harassment campaigns. Initially such attacks would be arson, vandalism and other forms of "monkey wrenching" – a term for sabotage combined with general mischief - but escalation is not only possible, it is likely. While claiming non-violence, letter-bombings and beatings have occurred in the course of these campaigns.

---

[184] Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999,* Report 0308, (Washington, D.C., n.d.), 27.
[185] Congress, House, Resources Subcommittee on Forests and Forest Health, *The Threat of Eco-Terrorism*, Statement by the FBI's Domestic Terrorism Section Chief, James Jarboe, (Washington, D.C., 12 February 2002), 1; available from http://www.fbi.gov/congress/congress02/jarboe021202.htm; Internet; accessed 17 January 2003; and Robert Gehrke, "FBI: Earth Liberation Front Most Active Domestic Terror Group," *Associated Press Newswires*, 12 February 2002, 1; available from http://www.stopecoviolence.org/pdfs/2_12_02.pdf; Internet; accessed 17 January 2003.
[186] "From Push to Shove," *Southern Poverty Law Center Intelligence Report,* no. 107 (Fall 2002), 4; available from http://www.splcenter.org/intelligenceproject/ip-index.html; Internet; accessed 17 January 2003.
[187] Craig Rosebraugh, "Craig Rosebraugh on the Anti-War Struggle," *Independent Media Center of Philadelphia*, 17 March 2003; available from http://www.phillyimc.org/article.pl?sid=03/03/17/2210240&mode=threat; Internet; accessed 29 April 2004.

Chart 5-2 below shows the increase in criminal acts by animal and environmental activists since 1981 as reported by the Foundation for Biomedical Research. The data shows a 148% increase in incidents during the decade of the 1990s over the previous decade and the number of incidents just in the first four years of the twenty-first century equal the total for the previous two decades combined.[188]

Chart 5-2: **Criminal Acts Committed by Animal Activists Against Plant and Animal Enterprises**
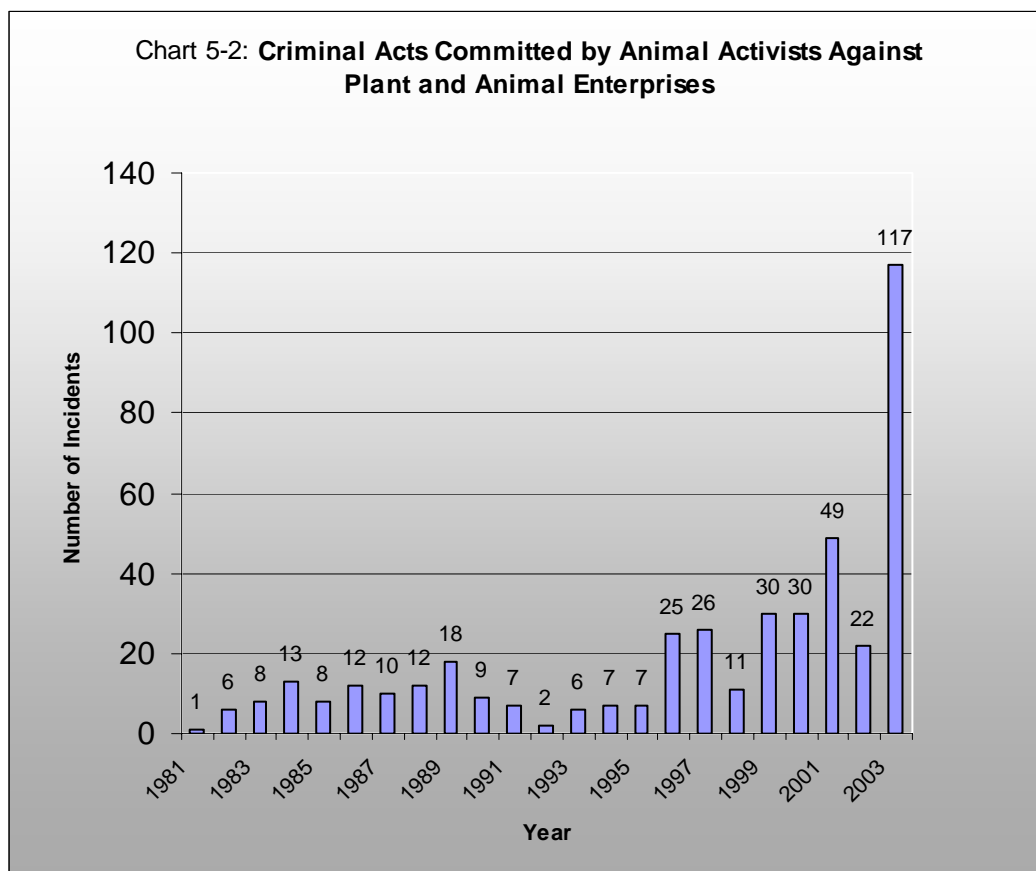
Possible Threats

Although not as likely as attacks or thefts to obtain military equipment, direct attacks on installations by radicalized domestic groups are possible. Objectives for such attacks are based upon the groups' perception of the U.S. Government as illegitimate or oppressive.

Some of these extremist domestic groups desire a "golden age" perceived by them in earlier U.S. history. This often centers around either increased states' rights or some strict, usually selective, interpretation of the U.S. Constitution. Traditionally "right-wing" groups have stepped up rhetoric and propaganda branding all government above county or state level as illegitimate. Ominously, much of the ideological material produced in this vein tends to

---

[188] *Illegal Incidents Summary* (Washington: Foundation for Biomedical Research, 2004), 3-39; available from; http://www.fbresearch.org/animal-activism/eventsummary.xls; Internet; accessed 29 April 2004.

dehumanize and advocate killing all nature of Federal Government servants, including and especially law enforcement and military personnel.

Lending credence to the possibility of these types of attacks, obvious symbols of Federal Government authority such as IRS facilities and Federal office buildings have been attacked repeatedly.[189] Despite the inherent drawbacks to terrorist targeting of military forces discussed in Sections II and III, the chances of some sort of attack occurring are increasing. Attacks have been discovered in the planning and preparation stage. Claims that control of the U.S. military has been usurped by hostile or conspiratorial foreign "forces" encourages the targeting of military facilities and personnel.

Domestic Threat To U.S. Army Installations
From "Terrorism in the United States, 1999" FBI Publication #0308, FBI

Between July 4 and July 11, 1997, the FBI, in conjunction with state and local law enforcement agencies in Texas, Colorado, Kansas, Indiana, and Wisconsin, executed multiple arrest and search warrants for a group of individuals planning an engagement with "foreign" troops stationed at the U.S. Army base at Fort Hood, Texas. The FBI was advised by undercover law enforcement officers that Bradley Glover, a self-proclaimed militia Brigadier General with a history of advocating the arrest of local law enforcement officers and members of the judiciary in Kansas, and an accomplice, named Michael Dorsett, anticipated an "engagement" with United Nations troops whom they believed were stationed at the military base. On July 4, 1997, after tracking the illicit activities of the two men, FBI Special Agents and officers from the Texas Department of Public Safety arrested Glover and Dorsett at Colorado Bend State Park, approximately 40 miles southwest of Fort Hood. Eight additional suspects were arrested and sentenced in Colorado, Kansas, Indiana, and Wisconsin for providing support to the operation.

Threats could also come from U.S. resident aliens or immigrant citizens with loyalties to ethnic, religious, or nationalist causes hostile to the U.S. or opposed to U.S. policies. As previously noted, these people may conduct operations as individuals or become operatives of existing groups. As "agents in place" – personnel already in the enemies' territory, and therefore less likely to be detected – they could be extremely dangerous and disruptive by merely working simple attacks as individuals or small cells. Modern information and telecommunications technology permits extensive linkages between immigrants and their home countries, and in some cases acts to preserve the individual's loyalty to the "homeland."

National Guard facilities and personnel are potential targets of attacks or sabotage to prevent counter-drug missions in support of local law enforcement. Since a significant amount of terrorist funding is obtained by drug manufacturing and smuggling, actions to prevent these missions or reduce their effectiveness could be in the terrorists' interests. However, these counter-drug missions would have to present a significant threat in order to provoke such attacks. Likewise, National Guard and Reserve members mobilized by their states or the Federal Government to increase security at high risk facilities in times of heightened alert may be targeted as a preemptive measure, or targeted as a statement by domestic groups against what they view as an encroaching "police state."

---

[189] Ibid., 52-61.

Preventative Measures

The heart of any program of preventive measures is denying the terrorist targeting information. Surveillance detection, OPSEC and counter intelligence activities all play a role in deterring and defeating terrorist operations. For the installation, the deployment of Military Police and other security elements is a flexible and responsive tool to react to increased threats. Coordination and liaison with local and Federal law enforcement is essential, as there will never be enough assets available to a post or activity to completely secure itself. Integration of existing guard posts, surveillance cameras, and other sensors into a network of coverage for the installation is a useful addition of capability to a protection plan. Similar coordination and liaison with civilian operators of critical infrastructure is just as important to ensure reliable services. The comments in Section III on access control and the ease of document counterfeiting apply to installations and activities even more than to units.

The terrorist can be affected by U.S. foreign or domestic policies, and political currents that are uncontrollable or unknown to the military members affected. Installations and activities may be targeted for symbolic reasons, in pursuit of social or political aims, in order to delay or destroy deployment capabilities, to destroy support and logistics infrastructure, to drain military resources into increased security versus war fighting, and to steal military equipment and weaponry. The potential attackers range from transnational terrorist organizations and state directed terror groups to individuals of no formal organization. Given the complex and pervasive nature of this threat, and the immense value of non-deployable forces to the military, terrorism is a challenge of tremendous proportions.

Conclusion

This chapter examined how U.S. military forces might be vulnerable to a myriad of terrorist activities. Whether military forces are deployed, deployable, or non-deployable, the potential operations conducted by terrorists are a constant threat to the military. Examples of specific terrorist operations indicate a wide range of tactics may be used to attack military units or installations. Preventive measures emphasize the importance of denying target information to the terrorist as a key to deterring and defeating terrorist operations.

Chapter 6
Future of Terrorism

> **All politics is a struggle for power…the ultimate kind of power is violence.**
> C. Wright Mills

Terrorism is evolving. While at the surface it remains "The calculated use of unlawful violence or threat of unlawful violence to inculcate fear…" it is rapidly becoming the predominant strategic tool of our adversaries. As terrorism evolves into a principal irregular warfare strategy of the twenty-first century, it is adapting to changes in the world socio-political environment. Some of these changes facilitate the abilities of terrorists to operate, procure funding, and develop new capabilities. Other changes are gradually moving terrorism into a different relationship with the world at large. However, terrorism and violence demonstrate a clear intention to gain power and influence in the future.[190] This chapter will examine the future of terrorism and the merging of terrorists with other state and sub-state entities. It will also examine some of the possible causes of future conflicts in order to understand the actors and their motivations. Finally, it discusses how terrorism will be integrated into this evolution of conflict, and what that will mean for U.S. military forces.

Section I: Future Trends in Terrorism

As a conflict method that has survived and evolved through several millennia to flourish in the modern information age, terrorism continues to adapt to meet the challenges of emerging forms of conflict, and exploit developments in technology and society. Terrorism has demonstrated increasing abilities to adapt to counter-terrorism measures and political failure. Terrorists are developing new capabilities of attack and improving the efficiency of existing methods. Additionally, terrorist groups have shown significant progress in escaping from a subordinate role in nation-state conflicts, and becoming prominent as international influences in their own right. They are becoming more integrated with other sub-state entities, such as criminal organizations and legitimately chartered corporations, and are gradually assuming a measure of control and identity with national governments. The FARC and ELN of Columbia depend on extortion, kidnapping, money laundering, and other economic strategies to finance their operations. Reports estimate that the FARC collects half a billion dollars per year from protecting the drug trade of the region.[191]

Other examples connecting criminals and terrorists exist in illicit cigarette trafficking. Recent years have witnessed a significant increase in this type of financing for terrorist activities. Known or suspected Hizballah and HAMAS members have established front companies and

---

[190] Bruce Harmon, *Inside Terrorism* (New York: Columbia University Press, 1998), 183.
[191] Christopher C. Harmon, Terrorism Today (London, Portland, OR: Frank Cass, 2000), 65 and 139.

legitimate businesses to cover an illegal market system, conduct money laundering, fraud, and tax evasion. Additionally, United States investigations have directly linked Hizballah and HAMAS to cigarette trafficking and material support to terrorism.[192] The United Kingdom knows that the Real IRA (RIRA) uses these techniques too. Government estimates state $30 million in fund raising for these type ventures by both sides of the sectarian violence in Northern Ireland.

Adaptive Capabilities of Terror Groups

Terrorists have shown the ability to adapt to the techniques and methods of counter-terror agencies and intelligence organizations over the long term. The decentralization of the network form of organization is an example of this. Adopted to reduce the disruption caused by the loss of key links in a chain of command, a network organization also complicates the tasks of security forces, and reduces predictability of operations.

Terrorists have also been quick to use new technologies, and adapt existing ones to their uses. The debate over privacy of computer data was largely spurred by the specter of terrorists planning and communicating over cyberspace with encrypted data beyond law enforcement's ability to intercept or decode this data. To exchange information, terrorists have exploited disposable cellular phones, over the counter long-distance calling cards, Internet cafes, and other means of anonymous communications. Embedding information in digital pictures and graphics and sending them over the Internet is another innovation employed to enable the clandestine global communication that modern terrorists require.[193] See the Cyber Operations appendix for more information on terrorist use of computer technology to support their operations.

Terrorists have demonstrated significant resiliency after disruption by counter-terrorist action. Some groups have redefined themselves after being defeated or being forced into dormancy. The Shining Path of Peru (Sendero Luminosa) lost its leadership cadre and founding leader to counter-terrorism efforts by the Peruvian government in 1993.[194] The immediate result was severe degradation in the operational capabilities of the group. However, the Shining Path has returned to rural operations and organization in order to reconstitute itself. Although not the threat that it was, the group remains in being, and could exploit further unrest or governmental weakness in Peru to continue its renewal.

In Italy, the Red Brigades (Brigate Rossi) gradually lapsed into inactivity due to governmental action and a changing political situation. This ultra-left wing terrorist group gained notoriety in the 1970s but had been effectively suppressed by the 1980s. In 1999, they resurfaced with the assassination of Italian government labor consultant Massimo D-Antona; in 2000, they murdered another labor consultant Marco Biagi. By late 2003, several group members had been arrested. Yet, a series of letter bombs were suspected as connected to the Red Brigade. Parcel bombs were mailed to the European Union (EU) president; bombs exploded in garbage cans near the EU president's home; letter bombs arrived at Europol, the

---

[192] William Billingslea, "Illicit Cigarette Trafficking and the Funding of Terrorism," *The Police Chief*, February 2004, 49-54.
[193] Thomas Homer-Dixon, "The Rise of Complex Terrorism", *Foreign Policy Magazine* (15 January 2002): 2.
[194] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Terrorism in Peru."

EUs police agency; and a letter bomb arrived at the European Central Bank in Frankfurt.[195] Also, a decade after the supposed demise of the Red Brigades, a new group called the Anti-Capitalist Nuclei emerged exhibiting a continuity of symbols, styles of communiqués, and potentially some personnel from the original Red Brigade organization. This ability to perpetuate ideology and symbology during a significant period of dormancy, and re-emerge under favorable conditions demonstrates the durability of terrorism as a threat to modern societies.

Increasing Capabilities

> **"Between now and 2015 terrorist tactics will become increasingly sophisticated and designed to achieve mass casualties."**
>
> National Intelligence Council
> "Global Trends 2015: A Dialogue About the Future With Nongovernment Experts" Report (Dec 2000).

Terrorists are improving their sophistication and abilities in virtually all aspects of their operations and support. The aggressive use of modern technology for information management, communication and intelligence has increased the efficiency of these activities. Weapons technology has become more available, and the purchasing power of terrorist organizations is on the rise. The ready availability of both technology and trained personnel to operate it for any client with sufficient cash allows the well-funded terrorist to equal or exceed the sophistication of governmental counter-measures.[196]

Likewise, due to the increase in information outlets, and competition with increasing numbers of other messages, terrorism now requires a greatly increased amount of violence or novelty to attract the attention it requires. The tendency of major media to compete for ratings and the subsequent revenue realized from increases in their audience size and share produces pressures on terrorists to increase the impact and violence of their actions to take advantage of this sensationalism.[197]

An indicator of this trend is the fact that terrorist incidents have been going down in total numbers since 1991, but the lethality per incident has gone up.[198] Chart 6-1 shows that the number of incidents began to rise in the early 1980s and peaked in 1987.[199]

---

[195] Francesco Di Meglio, "Italian Terrorists Generate Fear in Europe," *Italiansrus.com*; n.d.; available from http://www.italiansrus.com/articles/ourpaesani/redbrigade.htm; Internet; accessed 25 February 2004.

[196] Fred L. Fuller, "New Order Threat Analysis: A Literature Survey", *Marine Corps Gazette* 81 (April 1997): 46-48.

[197] *International Encyclopedia of Terrorism*, 1997 ed., s.v. "The Media and International Terrorism."

[198] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 200.

[199] Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2003* (Washington, D.C., April 2004, revised 22 June 2004), 176.

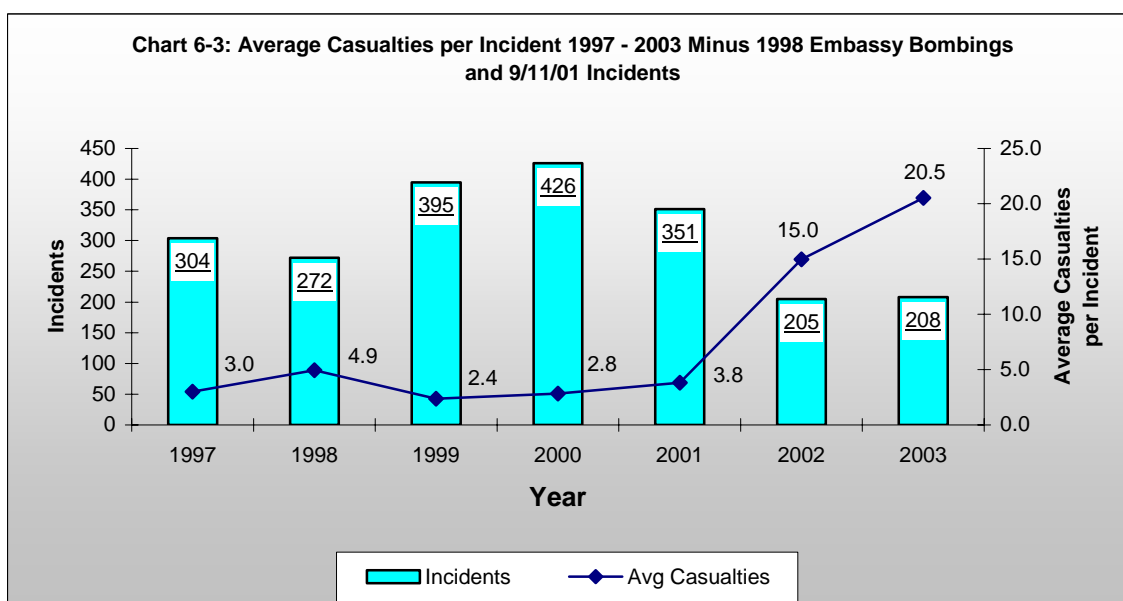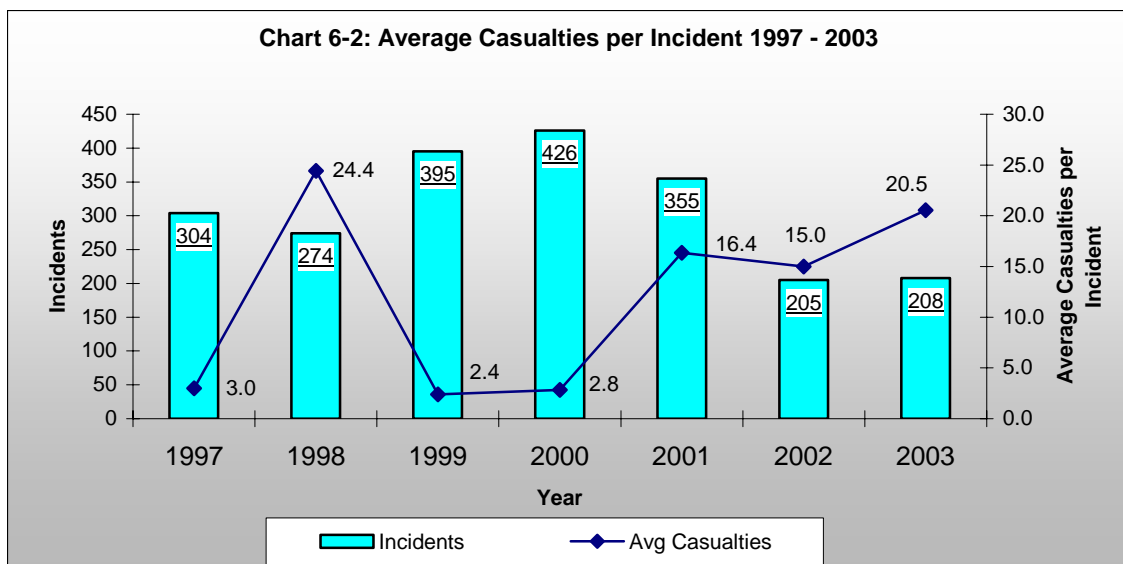**Chart 6-1: International Terrorist Attacks
1982 - 2003**
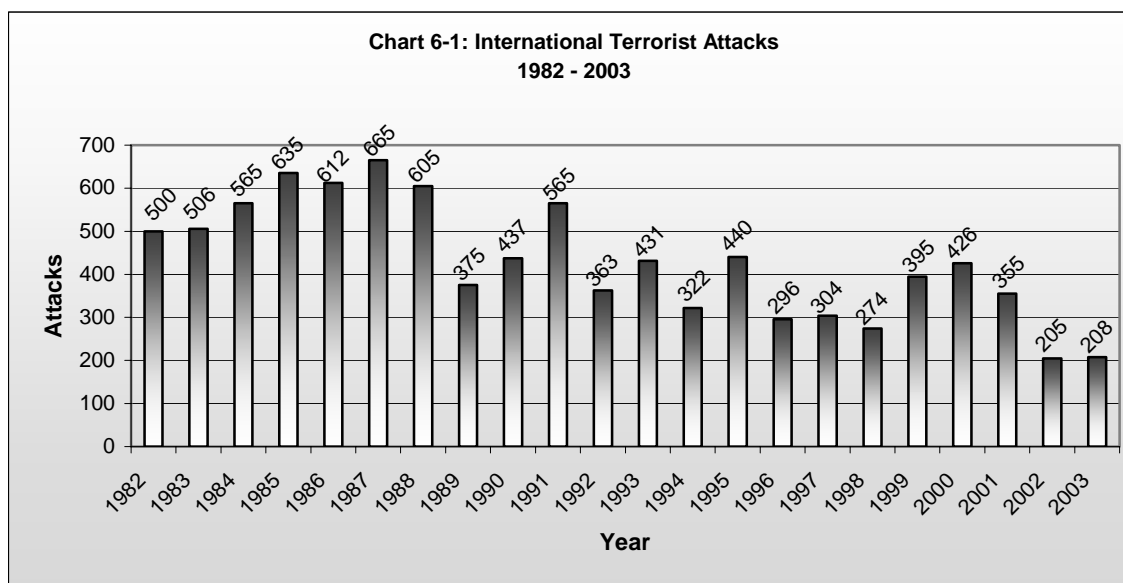
Since then the number of incidents has been declining. In fact, the years 2002 and 2003 have the fewest number of attacks during the 22-year period reflected on the chart. This is probably the result of both the war on terrorism and a conscious decision on the part of terrorist groups.

Fewer incidents with greater casualties appear to be the goal for many groups. This is not just a function of efficiency and developing skills, but also a tendency by the increasing number of religiously motivated groups to view ever-larger casualty lists as a measure of their influence and power. An ideal example of this attitude was the use of airliners as manned cruise missiles to strike the Pentagon and World Trade Center in September 2001. Chart 6-2 shows the average number of casualties per incident covering the period 1997 through 2003. As can be seen, the average number of casualties in 1997 was 3.0 per incident, whereas casualties in 2003 increased to 20.5 per incident. The years 1998 and 2001 show a large increase in the number of casualties per incident due to catastrophic events: the embassy bombings in Kenya and Tanzania in 1998 and the 9/11 incidents in 2001. These 3 events accounted for over 9000 casualties.

If the casualties from the embassy bombings of 1998, and the Pentagon and World Trade Center attacks in 2001 are removed from the data, as shown in Chart 6-3, the average casualties per incident in 2002 and 2003 indicate a significant increase in lethality over past years. There were no catastrophic events during these two years, but of the 413 incidents, 55 resulted in casualties of 30 or more, and 20 of the 55 resulted in casualties that exceeded 100.[200]

---

[200] Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2003* (Washington, D.C., April 2004, revised 22 June 2004), 95-112; and *Patterns of Global Terrorism 2002* (Washington, D.C., April 2003), 83-98.

Chart 6-2: Average Casualties per Incident 1997 - 2003

Incidents by year: 1997: 304; 1998: 274; 1999: 395; 2000: 426; 2001: 355; 2002: 205; 2003: 208

Average Casualties: 1997: 3.0; 1998: 24.4; 1999: 2.4; 2000: 2.8; 2001: 16.4; 2002: 15.0; 2003: 20.5

Legend: Incidents — Avg Casualties

Chart 6-3: Average Casualties per Incident 1997 - 2003 Minus 1998 Embassy Bombings and 9/11/01 Incidents

Incidents by year: 1997: 304; 1998: 272; 1999: 395; 2000: 426; 2001: 351; 2002: 205; 2003: 208

Average Casualties: 1997: 3.0; 1998: 4.9; 1999: 2.4; 2000: 2.8; 2001: 3.8; 2002: 15.0; 2003: 20.5

Legend: Incidents — Avg Casualties

The trend to exploit available technologies and the desire for more casualties will probably accelerate the eventual employment of Weapons of Mass Destruction (WMD) by terrorists. Documented uses of chemical (Tokyo 1995) and biological weapons (Oregon in 1984[201] and Florida and Washington D.C. in 2001) have already occurred and as mentioned earlier in this handbook, al Qaeda has stated that it is their intent to acquire WMDs.

---

[201] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 121.

Escaping Dependence

During the evolution of modern terrorism in the Cold War era, even nationalist insurgent groups sought out, indeed required, a sponsor from one of the two competing ideological blocs. These sponsors could effectively influence the policy of their clients, and exercise a limited form of control over their actions. This gradually shifted to a less rigid control as more sponsors, such as Libya, entered the field. The death of the bipolar world order removed both the motivations and capabilities of a large number of state sponsors. This loss of significant resources eliminated many terrorist groups; particularly those closely aligned with the communist bloc, and increased the costs for sanctuary and training for many others.[202]

In addition, punitive actions against "rogue states" have gradually shut down some geographical sanctuaries and sources of support for terrorists. Although this can be temporarily disruptive, new players will replace the old. Groups based in Libya shifted to Iraq or Syria when support was restricted due to international sanctions and U.S. military action against Libya because of their sponsorship of terrorism. Similarly, al Qaeda shifted key functions from the Sudan to Afghanistan when U.S. action and diplomatic pressure were brought to bear in that geographical area.

In response, terrorists have adjusted their financial operations to become more self-sustaining in their activities, resulting in greater independence from any external control. Terrorist operations require extensive financial support. The facility with which groups can obtain and move funds, procure secure bases, and obtain and transport weaponry determines their operational abilities and the level of threat that they pose. The international nature of finance, the integration of global economies, and the presence of terrorists in the illegal "black" economies of slaves, drugs, smuggling, counterfeiting, identity theft, and fraud have aided this new independence from traditional sources of sponsorship and support.[203]

This evolutionary development has inverted the previous relationship between terrorists and governments.[204] In the earlier relationships, the nation-state sponsor had some measure of control. Due to the ability of terrorist groups to generate tremendous income from legitimate and illegal sources, it often becomes the terrorist organization that "sponsors" and props up its weaker partner, the national government. For example, during the period it was based in Afghanistan, al Qaeda was running an annual operating budget of approximately $200 million, while their hosts, the Taliban had only $70 million annually.[205] In addition to financial supremacy, al Qaeda personnel also provided much of the technical expertise the Taliban lacked. The only asset the Taliban had to offer was sanctuary and the advantages their status as a recognized national government provided in some countries.

---

[202] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 3.

[203] Kimberly L. Thachuck, "Terrorism's Financial Lifeline: Can it Be Severed," *Strategic Forum* no. 191 (May 2002): 2.

[204] Maurice R. Greenberg, Chair, William F. Wechsler and Lee S. Wolosky, Project Co-Directors, *Terrorist Financing: Report of an Independent Task Force Sponsored by the Council on Foreign Relations* (New York: Publication Office, Council on Foreign Relations, 25 November 2002), 5.

[205] David Albright, "Al Qaeda's Nuclear Program: Through the Window of Seized Documents," *Policy Forum Online* Special Forum 47 (6 November 2002): 8; available from http://www.nautilus.org/fora/Special-Policy-Forum/47_Albright.html; Internet; accessed 14 February 2003.

Although the explosion in terrorist income has been tied to the increasing involvement of terrorists in international crime, simpler support by the more traditional means of donations, extortions, and extra-legal contributions can be leveraged into significant sums through investment. The PLO is an excellent example of financing through legitimate investments. The organization managed to acquire sufficient wealth by these means in the 1980s, receiving an estimated 80% plus of its annual operating budget of $600 million from investments.[206] This allowed the PLO progressively greater autonomy in dealing with other nations.

Merging Identities

Terrorist groups and other illegal sub-state organizations are rapidly becoming indistinguishable from each other. The increasing role of criminal activity in financing terrorism, either in partnership or competition with traditional criminal activities, is making it

> **"States with poor governance; ethnic, cultural, or religious tensions; weak economies; and porous borders will be prime breeding grounds for terrorism. In such states, domestic groups will challenge the entrenched government, and transnational networks seeking safe havens."**
>
> "Global Trends 2015: A Dialogue About the Future With Nongovernment Experts" Report (December 2000).

very difficult, if not impossible, to clearly determine where one stops and the other begins. These enterprises include well-publicized activities such as drug trafficking and smuggling, which some terrorists, insurgencies, and even less reputable governments have been engaged in for decades. They also include newer, less well-known illegal activities such as welfare fraud, tax evasion and fraud, counterfeiting, and money laundering. Many of these activities are offshoots of terrorist groups' evolving capabilities of false documentation and concealment of money transactions for their operational purposes. These activities now generate a profit for additional funding.

Terrorists and criminal organizations are becoming more closely related, as terrorists utilize criminal networks and methods to operate, and as criminals become more politicized.[207] As national governments fail, their ruling elites frequently criminalize the nation itself, lending their sovereignty to smuggling, money laundering, piracy, or other illicit activities. Their security forces may retreat into terrorism to hold onto what power or authority they can, and use terrorist groups to function in place of the official arms of the government. Successful coups often generate governments that immediately resort to terror to consolidate their position.[208]

---

[206] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 84.

[207] "The New Threat of Organized Crime and Terrorism" *Jane's Terrorism & Security Monitor* (6 June 2000): 1-5; available from http://www.janes.com/security/international_security/news/jtsm/jtsm000619_1_n.shtml; Internet; accessed 27 June 2000.

[208] Robert Kaplan, *The Coming Anarchy: Shattering the Dreams of the Post Cold War* (New York: Random House, 2000), 48.

This interpenetration of a criminal element into the government while government officials are "seeping" down to the terrorists' level is the result of governments feeling that legality, in the international sense, is a luxury they cannot afford, and perhaps do not need. They lack the resources to adhere to "legalistic" notions, and thus sink into criminality. The better-funded sub-state organizations (terrorist, criminal, etc.) infiltrate or supplant the government. Eventually, there is no distinction between the two as they effectively merge. The situation in Liberia at the start of the twenty-first century is an excellent example of this phenomenon.

A development related to this is the emergence of "gray areas"; those places where no government exercises actual control, and any order is imposed by sub-state, usually criminal organizations. Militias, traffickers, mafias, and terrorists operate their own fiefdoms, either as coalitions or in various states of coexistence ranging from truce to open hostility. These "gray areas" may be ungovernable slums or shantytowns in urban centers, or rural stretches too far away from the central government for effective control.[209]

Section II: The Future of Conflict

Whether you view the post-Cold War world with alarm or optimism, it is clear that there will be future conflicts. There are more unresolved international issues left over from the forty-plus years of the Cold War than from the conclusion of either of the two World Wars. However, now there is no "balance of power" or two-power system to regulate the conflicts that will arise from these issues. Finally, the types of issues, and the antagonists involved with them, have fundamentally shifted. The nation-state system is showing signs of erosion in many parts of the globe, and a return to the days of mercenary chieftains and small city-states is already underway in some areas of the world.

In this section we will look at what will inspire conflicts in the twenty-first century, and what some of the differences from the existing pattern will be. We will then look at some of the resulting practical impacts on the use of terrorism against U.S. forces.

Future Conflicts

The world order has changed significantly. The number of new, sovereign nations that emerged from the end of the Cold War rivals the new nations created after the two World Wars and the retreat of the colonial empires in the 50s and 60s. However, not all of these nations are viable states and most of them do not have stable leadership other than that of local ethnic or tribal strongmen. Many have significant problems aside from poor leadership, especially in the developing world. The most significant of these problems include:

- Disease

- Resource Depletion

- Factionalism

---

[209] Xavier Raufer, "New World Disorder, New Terrorisms: New Threats for the Western World," in *The Future of Terrorism*, ed. Max. Taylor and John Horgan (Portland: Frank Cass Publishers, 2000), 32.

<u>Disease</u>: The incidence of newer pandemics such as HIV/AIDS and Ebola are just now beginning to equal the lethality of older scourges such as plague, malaria and other tropical fevers. The World Health Organization reports 1,000 to 3,000 cases of plague every year.[210] On the other hand, the 2004 United Nations report on AIDS reports almost five million new cases of HIV in 2003.[211]   Further, both HIV/AIDS and Ebola are concentrated in the developing nations of the world, where the metamorphosis of productive populations into invalids exacerbates the health-care costs these diseases inflict. Particularly in Africa and Southeast Asia, countries are seeing their populations decimated in their most productive years. Gene research and the field of genomics may help combat new diseases, but offer the potential of a two-edged sword. Although it may provide advances in health care, it could also acquire a perverse tack toward biological warfare with very specific infections and target groups.[212]

<u>Resource Depletion</u>: Those countries that lack a base of sufficient industrial or technological production to sustain an economic system fall back on basic agriculture and resource extraction. However, population pressure and lack of foresight encourage rapid depletion of finite resources. The result is further degradation of the economy, with nothing to show for it in the way of infrastructure improvement or alternative production. The establishment of a viable economic system to support a national government becomes impossible, and what little economic activity is possible is usually conducted illegally.

<u>Factionalism</u>: Many nations resulting from the post-colonial era are simply geographic "fictions." They are reminders of an earlier power system on a map, lacking any sense of national or geographic identity, and driven with tribal and ethnic divisions. Africa is a particular case in point, with national boundaries being the result of colonial influences, not indigenous tribal identities. The tensions between factions, and the attraction for a minority in one country to join with their ethnic brothers who are a majority in a nation next door, is a destabilizing influence on many nations. Lacking a cohesive identity, other pressures eventually cause weak states to splinter, or gradually pull apart.

In a related development non-state and sub-state organizations and power blocs are assuming military roles and utilizing organized forces in conflicts, and terror tactics in socio-political conflicts. Major corporations, private security companies, and well-funded transnational terror groups have all played kingmaker in failed or dysfunctional states in the last decade. In some cases parts of the world are returning to a pre-nation-state condition as non-state actors, capable of challenging or disrupting governments and nations, are emerging in the "gray areas."

---

[210] "Plague," *CDC Plague Home Page;* available from http://www.cdc.gov/ncidod/dvbid/plague/index.htm; Internet; accessed 9 July 2004.

[211] *2004 Report on the Global AIDS Epidemic: Executive Summary* (Geneva: Joint United Nations Programme on HIV/AIDS, 2004), 5.

[212] "In My Humble Opinion: Genomics is the most important economic, political, and ethical issue facing mankind," *Fast Company*, November 1999; available from http://www.fastcompany.com/online/29/jellis.html; Internet; accessed 26 February 2004.

Inevitability of Conflict

Because of the widespread instability resulting from the problems noted above, a multitude of small to medium conflicts are inevitable. There are two likely models regarding the fundamental nature of these future conflicts, and while they are not mutually exclusive, they emphasize different things. The first model is strategic in nature, and holds that past conflicts have moved gradually upward in level from tribal to national to ideological struggles, culminating with World War II and the Cold War. The next conflicts will be between cultures.[213] This view predicts fighting along the parts of the world where cultures intersect, such as the Central Asian confluence of the Islamic and Eastern Orthodox cultures. The assumption is that wherever there is a line of engagement between two differing cultures, there will be conflict.

In light of this view, a transnational network like al Qaeda becomes more than a fundamentalist religious terror movement, whose goal of replacing the power structures in the historical Arab world with a new Caliphate is impractical and unlikely. When viewed at this "clash of cultures" level, al Qaeda becomes a true transnational insurgency, fighting against imposed Western political ideals and alien social order across multiple countries and regions simultaneously. Stateless for the moment, much as the early Communist revolutionaries before the Russian Revolution, these cadres hope to organize the vanguard of a religious revolution whose eventual success they consider inevitable.

The second model predicts the failure of significant numbers of the current nation-states in the developing world. Unable to overcome such challenges as depleted resources, disease, and ineffective leadership, there is no way for these countries to become viable. Unable to exert authority, protect their citizens, or control their borders, they are disintegrating. Many of these countries are splintering into tribal and ethnic factions that might coalesce into a new, more stable form, or continue to devolve through violence into lawless zones of minor warlords and bandits.[214]

Regardless of which model more accurately describes the future, a most important occurrence common to both will be the blurring and blending of terrorists as we now categorize them with other groups that will resort to force and violence to achieve their aims. As discussed at the end of Section I, the expansion of "gray areas" and the criminalizing of what remains of the nation-state could likely render parts of the world essentially "no-man's land" in terms of our currently understood international system.

How Changes Impact Terrorism and U.S. Forces

Terrorism has generally seen success as a tactic and failure as a strategy. Many of the emerging entities that are rising to wield effective power in failing states are only concerned with the immediate tactical effects of their actions. They therefore look upon modern

---

[213] Samuel Huntington,"The Clash of Civilizations," *Foreign Affairs* (Summer 1993): 2; available from http://www.lander.edu/atannenbaum/Tannenbaum%20courses%20folder/POLS%20103%20World%20Politics/103_huntington_clash_of_civilizations_full_text.htm#I.%20THE%20NEXT%20PATTERN%20OF%20CONFLICT; Internet; accessed 6 December 2002.
[214] Robert Kaplan, *The Coming Anarchy: Shattering the Dreams of the Post Cold War* (New York: Random House, 2000), 7-9.

terrorism as an effective mode of conflict. They can point to the fact that al Qaeda invested $500,000 in an attack that is estimated to eventually cost the U.S. Government $135 billion in damages and recovery costs.[215] Considering that these figures do not reflect the costs of military and law enforcement efforts to investigate and destroy the organization responsible, the comparative return on the investment is even greater.[216]

Since these emerging and sub-state entities are not party to any established rules regarding the uses of force, terrorism and the use of terror to oppress are viewed as logical and effective methods to accomplish their objectives. The development of rules of war and the framework of international laws that attempt to protect the civilian from military action are irrelevant to these combatants. Thus the expansion of where and to whom violence may be applied will accelerate, and the treatment of prisoners will rely more on the provision for ransom or retribution for mistreatment than on the rulings of the Geneva Convention.[217]

This is important for the unit leader and planner because the mind set necessary to operate in a completely chaotic, unstructured environment will have to be developed. This mind set includes the sobering, and for Americans, unusual, concept that their units may likely be the only order or structure in their area of operations. There will be no "host nation government" and perhaps no local government. If there is any government at all, there very well may be several, all claiming some degree of legitimacy, and potentially all of which could be hostile.[218] U.S. forces deployed in these environments will constitute mobile capsules of order and structure, but that order will disappear after they pass through the area.

Although this sounds as if all future operations will be attempts to impose order or stability against sub-state adversaries, and implies that major conventional conflict is a thing of the past, there is another possibility. There are theories for using all of these levels of disorder, as well as economic warfare, information warfare, and conventional military force, in an orchestrated campaign against an adversary. This would be conducted as a long-term effort of undeclared conflict that might appear as amicable relations between the two adversaries, but with one pursuing the eventual defeat of the other through multiple, simultaneous methods.[219] Forms of terrorism easily fit into this construct of overt and covert conflict. The arena of cyber-war exemplifies the ability to impact on critical infrastructure, and its disruption and damage to national security, economic functions, and U.S. military response.[220]

The effectiveness of this approach is in the costs to the victim to defend against multiple threats with no clear foe. Operational control over the various "tools" employed by the aggressor is not required, as long as the "tools" perform their role of bleeding the adversary of resources and resolve. Deniability is maintained and diplomacy pursued to keep the

---

[215] Kimberly L. Thachuck, "Terrorism's Financial Lifeline: Can it Be Severed," *Strategic Forum* no. 191 (May 2002): 4.

[216] Fred L. Fuller, "New Order Threat Analysis: A Literature Survey", *Marine Corps Gazette* 81 (April 1997): 46-48.

[217] Martin L. Van Creveld, *The Transformation of War* (New York: The Free Press, 1991), 202.

[218] Robert Kaplan, *The Coming Anarchy: Shattering the Dreams of the Post Cold War* (New York: Random House, 2000), 47.

[219] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare,* trans. Department of State, American Embassy Beijing Staff Translators (Washington, D.C., 1999).

[220] President,*The National Strategy to Secure Cyberspace.* (Washington, D.C., February 2003), Preface; available from http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf; Internet; accessed 8 December 2003.

conflict from becoming focused before the aggressor is ready. Although all manner of unconventional threats may be employed, terrorism is a key component of this strategy.

On the practical level, what changes to terrorist operations will concern U.S. forces? As already addressed, terrorism will continue to increase in lethality. The acquisition and eventual use of effective WMDs by terrorists is highly likely. Terrorism is merging and combining with various other state and sub-state actors, further blurring the difference between criminals, rogue governments, and terrorists.

There are several practical considerations in the evolution of terrorism that have not yet been addressed. These are concerns regarding the impacts and interactions of mass media, technological advances, urbanization, and illegal fundraising with terrorism.

There is an increasingly technological and informational nature to all conflict, and terrorism is no exception. Terrorists will continue to cultivate their ability to use new and innovative technologies, and methods of applying existing technologies to new uses. This is not to say that terrorists will go exclusively "high-tech," but they will explore the increase in capabilities that technology provides, especially the synergy between simple operations and selective technologies to ensure success. There is no doubt that terrorists will continue to exploit information technology to enhance their operations and to launch cyber attacks against our IT systems.

Terrorists will attempt to exploit U.S. vulnerabilities to information dominance. Casualty avoidance and the "CNN" effect are interrelated perceptions held by many potential adversaries of the U.S. socio-political situation. Most of our adversaries believe the U.S. is extremely casualty averse, and that images and news of casualties will be easy to deliver to American living rooms. This image has been reinforced by the news media's coverage of casualties in both OEF and OIF. While this effect may be overemphasized, we should expect it to be a significant part of terrorist planning and targeting.

In the techniques of the "CNN war," terrorists were pioneers.[221] Since the terrorists prepare their operations around the desired media effect, they will always be out in front of the reporting. They will orchestrate supporting events and interviews to reinforce the desired message. Terrorists have well-established methods of presenting disinformation and false perspectives. The use of "spin" has become widespread, and is relatively successful. Frequently, military reluctance to comment on ongoing operations in the media for OPSEC reasons can play into the hands of the terrorist, as there will be no balancing information from official sources for hours or days after an incident, leaving the terrorist message as the only one in play.

Terrorists will exploit the vulnerabilities of new technologies to attacks or disruption. Terrorists have a great deal of flexibility in their ability to acquire new technology. The historical vignette of the Fenian Ram (see text box below) shows how the application of innovative technology to a specific target eliminates the advantages held by conventional military forces. They also have the advantage of only needing to attack or neutralize specific systems or capabilities. Consequently, they can narrowly focus their expenditures on the

---

[221] Bruce Hoffman, *Inside Terrorism* (New York: Columbia Universty Press, 1998), 133-139.

limited counter-technology they need. Also, they can neutralize some advanced systems or capabilities through the use of innovative and unconventional techniques, such as the employment of suicide bombers.

Modern, high-technology societies are susceptible to a "complex terrorism." Dependence on electronic networks, sometimes with minimal redundancy, and concentrating critical assets in small geographic locales can present lucrative targets for the terrorist. Ensuring redundant systems exist, dispersing critical assets physically, and creating buffers, firewalls, or other type safeguards can enhance defense and recovery from such complex terrorist attacks.[222]

There are potential cyber-terrorism impacts here in relation to the U.S. military transformation. As the U.S. military increases its battlefield information capabilities, vulnerabilities peculiar to networks such as overload feedback between nodes and destruction of key concentration nodes become available for terrorists to exploit.[223] Deception techniques exploiting our reliance on technology have already been used with some success.[224] When Usama bin Laden thought American satellites were being used to locate him tracing his satellite phone, he had an aid depart from his location carrying the phone. Evidently the aid was captured with the phone, while bin Laden escaped.

The military will not be the only, or necessarily the primary target of new strategies useful against leading edge technologies and organizations. The dispersal of key civilian infrastructure nodes into locations remote from the urban complexes they serve increases their vulnerability and the reliance on computerized control systems to monitor and control these nodes increase their exposure to cyber-terrorism.

Participation in and use of terrorism will increase. Individuals and groups that are not currently employing terrorism will adopt it as a tactic, and those that are employing terror tactics at low levels of lethality will become more violent. This is a combination of existing terrorist groups trying to destabilize the existing order on an ever-widening basis, and the previously discussed tendency of terrorist groups to increase the level of violence when not immediately successful.[225]

Terrorist basing and operations in urban environments will increase. Terrorists have typically operated in urban environments, but the emergence of "megalopolis" cities in undeveloped or poorly developed countries, with poor services, weak governance, and rampant unemployment and dissatisfaction has created a near perfect recruiting ground-cum-operating environment for terrorists. Many of these cities have adequate international communication and transport capacities for the terrorists' purposes; yet have ineffective law enforcement and a potentially huge base of sympathizers and recruits. The inability of external counter-terror

---

[222] Thomas Homer-Dixon, "The Rise of Complex Terrorism," *Foreign Policy Magazine* (January-February 2002): 1, 6, and 7; available from http:// www.foreignpolicy.com/story/cms.php?story_id=170; Intenet; accessed 26 August 2004.
[223] Ibid., 3-4.
[224] "Osama's Satellite Phone Switcheroo," *CBS News.com,* 21 January 2003, 1; available from http://www.cbsnews.com/stories/2003/01/21/attack/main537258.shtml; Internet; accessed 10 February 2003.
[225] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 162-163.

and law enforcement organizations to effectively intervene where the local government is unable to assert authority is another advantage.[226]

Vignette: 19th Century Technology & Terrorism
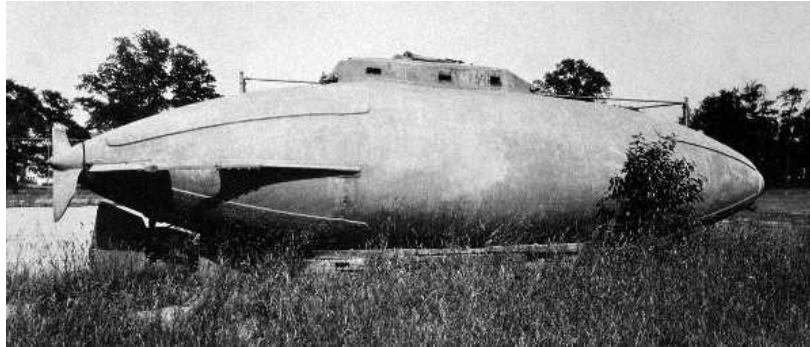
The Fenian Ram at the New York State Marine School (1916-1927)

John Holland   (*Source:* Photos Courtesy of US Navy)

The threat of cutting edge technology in the hands of terrorists is not unique to the modern era. What was arguably the first practical modern submarine design was commissioned by the Fenian Brotherhood to sink British warships. The Brotherhood was an Irish nationalist movement active in the U.S. and Britain in the late 19th century. In addition to assassinations and bombings, they conceived several bold projects to strike at the British, not least of which were two attempted invasions of Canada, with the goal of holding the Dominion hostage for Irish independence.

A more feasible, but still daring project was the construction of a submarine capable of sinking Royal Navy warships. Designed by John Holland, and launched in 1881, the *Fenian Ram* carried a crew of three and could operate up to 45 feet beneath the surface. Holland was an Irish immigrant to the U.S. whose brother Michael was involved with the Brotherhood, and financed his design and construction efforts. The submersible would be delivered to the target area by an innocent looking merchant ship. Using a compressed air gun to launch 100-pound dynamite projectiles several hundred yards, the *Ram* would attack with complete surprise, and escape submerged.

The Fenians' selection of the Royal Navy as the target shows a keen appreciation of the psychological effects of terrorism. While Holland hoped for a military role for his invention, and later worked with the U.S. Navy, the Fenians' regarded it as a more sophisticated way to place a bomb. Britain's fleet was absolutely essential to the security and maintenance of the far-flung empire, and was also a national institution of great tradition and pride. A successful campaign using the *Ram* and others like it would have been a tremendous blow to both the security and prestige of Britain.

The Ram was stolen by the Brotherhood in 1883 in a dispute over money. Although they had the vessel, they were not familiar enough with it to operate it, and it was never used. John Holland continued with his experiments, and his eventual design became the basis for the submarines used by the U.S., Netherlands, and Japanese navies, among others. Ironically, the Royal Navy's first submarines were manufactured from Holland designs. Admiral Sir Arthur Wilson may have known about the designers' original intent when he pronounced submarines, including those of the British Royal Navy, as "…underwater, underhanded, and damned un-English".

---

[226] Xavier Raufer, "New World Disorder, New Terrorisms: New Threats for the Western World," in *The Future of Terrorism*, ed. Max Taylor and John Horgan (Portland: Frank Cass Publishers, 2000), 32.

The advantage to terrorist organizations that use criminal activities to fund operations will continue to grow. Money is the great force multiplier for terrorists, and criminal activity produces more money than other strategies. The annual profit from criminal activity is estimated at 2-5% of the world Gross Domestic Product, or $600 billion to $1.5 trillion *in profit.*[227] Terrorists are emphasizing criminal activities for their support funding because it allows them to compete more effectively with their adversaries, and conduct larger and more lethal operations.

Conclusion

This final chapter examined the future of terrorism, with emphasis on the integration of terrorism with concepts of world disorder and new forms of conflict. The evolution of today's terrorist into a non-state "politicized criminal" is an arena of growing concern. The merging of criminals, rogue political leaders, and terrorists into one collective identity, which operates to realize economic and political power, is a possibility. The United States will have to adapt to modes and states of conflict we have been traditionally uncomfortable with, but can now no longer ignore.

---

[227] Kimberly L. Thachuck, "Terrorism's Financial Lifeline: Can it Be Severed," *Strategic Forum* no. 191 (May 2002): 2.

Page Intentionally Blank

Appendix A
Terrorist Threat to Combatant Commands

U.S. interests are spread throughout the world. So, every Muslim should carry out his real role to champion his Islamic nation and religion. Carrying out terrorism against the oppressors is one of the tenets of our religion and Shari'ah.

Al Qaeda Statement, October 10, 2001

General

In 2002, the Secretary of Defense and Chairman of the Joint Chiefs of Staff announced the 2002 Unified Command Plan, which established five Combatant Commands:

- U.S. Northern Command (USNORTHCOM)
- U.S. Southern Command (USSOUTHCOM)
- U.S. Pacific Command (USPACOM)
- U.S. European Command (USEUCOM)
- U.S. Central Command (USCENTCOM)

Figure A-1. The World with Commanders' Areas of Responsibility

---

[228] Department of Defense, *Special Briefing on the Unified Command Plan*, by Donald H. Rumsfeld, (Department of Defense News Briefing Transcript presented at the Pentagon, Wednesday, 17 April 2002 – 11:30a.m); available from http://www.defenselink.mil/news/Apr2002/t04172002_t0417sd.html; Internet; accessed 18 November 2002.

This appendix addresses the terrorist threat facing each one of these commands. Each Combatant Command Area of Responsibility (AOR) is listed reflecting the terrorist groups that are physically based within it, plus other groups that either have a presence or have operated within the AOR. We must realize, though, that any terrorist group that has the manpower and financial resources can operate within an AOR if its objectives dictate an operational requirement to do so. Imminent danger to U.S. military forces can change rapidly. Not all groups listed will profess to target U.S. interests, but all listed could easily do so.

This material should be considered suitable for general orientation. Since the information on terrorist groups is dynamic and changes frequently, actual planning and threat assessments should utilize appropriate intelligence products from the commands listed. The major input for this section comes from the United States Department of State report entitled: "Patterns of Global Terrorism 2003", dated April 2004[229] (located at http://www.state.gov/s/ct/rls/pgtrpt/2003/), and the Center for Defense Information list of known terrorist organizations[230] (http://www.cdi.org/terrorism/terrorist-groups-pr.cfm). Information listed for USNORTHCOM was also obtained from the FBI publication, *Terrorism in the United States 1999*[231] (located at http://www.sas.org/Terrorist/archive/FBIterror99.pdf) and the *Historical Dictionary of Terrorism.*[232] An * indicates past history of anti-U.S. activity.

U.S. Northern Command

Groups Physically Based In AOR	Strength	Anti-U.S. Activity
*Animal Liberation Front (ALF)**	Unknown	Yes
*Aryan Nations**	150 – 500	Yes
*Christian Identity affiliated groups**	Varies	Yes
*Earth Liberation Front (ELF)**	Unknown	Yes
*Fuerzas Armadas de Liberacion Nacional Puertorriquena (Armed Forces for Puerto Rican National Liberation (FALN)**	< 50	Yes
*Jamaat ul-Fuqra**	200	Yes
*Ku Klux Klan affiliated groups**	9,000 – 20,000	Yes

---

[229] Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2003* (Washington, D.C., April 2004, revised 22 June 2004), 113-160.

[230] Christopher Hellman and Reyko Huang, *List of Known Terrorist Organizations* (Washington: Center for Defense Information Terrorism Project, 2001), 1-31; available from http://www.cdi.org/terrorism/terrorist-groups-pr.cfm; Internet; accessed 24 October 2002.

[231] Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999,* Report 0308, (Washington, D.C., n.d.), 50-51.

[232] Sean K. Anderson & Stephen Sloan*, Historical Dictionary of Terrorism* (Lanham, MD: Scarecrow Press, Inc, 2002).

*Loosely affiliated ad hoc groups**	Varies	Yes
*Los Macheteros (Puerto Rico)**	< 40	Yes
*Militias/Patriot/Conspiracy affiliated groups**	Varies	Yes
*Neo-Nazi affiliated groups**	Varies	Yes
*Posse Comitatus groups**	1,000 – 3,000	Yes
*Skinhead affiliated groups**	2,500 – 3,500	Yes
*World Church of the Creator (WCOTC)**	Unknown	Yes

Table A-1. Terrorist Groups Based in USNORTHCOM

Other Groups Operating or with Presence in the AOR	
*Al-Gama'a al-Islamiyya (IG)**	*Japanese Red Army (JRA)**
*Al Qaeda**	*Kach*
Cambodian Freedom Fighters (CFF)	*Kahane Chai*
HAMAS	*Manuel Rodriquez Patriotic Front (FPMR)**
*Hizballah**	*Mujahedin-e Khalq Organization (MEK)**

Table A-2. Terrorist Groups with Presence in USNORTHCOM

U.S. Southern Command

Groups Physically Based In AOR	Strength	Anti-U.S. Activity
*Manuel Rodriquez Patriotic Front (FPMR), (Chile)**	50 - 100	Yes
*Morzanist Patriotic Front (FPM), (Honduras)**	Unknown (Est. small)	Yes
*National Liberation Army (ELN), (Colombia)**	3,000	Yes
*Revolutionary Armed Forces of Colombia (FARC), (Colombia)**	9,000 – 12,000	Yes
*Sendero Luminoso (Shining Path) (SL), (Peru)**	400 – 500	Yes
Tupac Amaru Revolutionary Movement (MRTA), (Peru)	≤100	None
United Self-Defense Forces/Group of Colombia (Autodefensas	8,000 – 11,000	None

Unidas de Colombia) (AUC), (Colombia)		

Table A-3. Terrorist Groups Based in USSOUTHCOM

Other Groups Operating or with Presence in the AOR	
Al-Gama'a al-Islamiyya (IG)*	Irish Republican Army (IRA)
Al Qaeda*	Mujahedin-e Khalq Organization (MEK)*
Hizballah*	

Table A-4. Terrorist Groups with Presence in USSOUTHCOM

U.S. European Command

Groups Physically Based In AOR	Strength	Anti-U.S. Activity
Al-Aqsa Martyrs Brigade,(al-Aqsa), (Occupied Territories)*	Unknown	Yes
Allied Democratic Forces (ADF), (Congo)(Listed in the 2002 State Department Report – Deleted in 2003)	Few hundred	None
Anti-Imperialist Territorial Nuclei (NTA), a.k.a.: Anti-Imperialist Territorial Units, (Italy)*	20	Yes
Armed Islamic Group (GIA), (Algeria)	Unknown (Est. < 100)	None
Army for the Liberation of Rwanda (ALIR), a.k.a.: Interahamwe, Former Armed Forces of Rwanda (ex-FAR), (Rwanda)*	Unknown (Several thousand operate in eastern DRC)	Yes
'Asbat al-Ansar (The League of the Followers), (Lebanon)*	300	Yes
Basque Fatherland and Liberty (ETA), a.k.a.: Euzkadi Ta Askatasuna, (Spain)	Unknown (Est. several hundred)	None
Continuity Irish Republican Army (CIRA), a.k.a.: Continuity Army Council, (Northern Ireland)	< 50	None
Democratic Front for the Liberation of Palestine (DFLP), (Occupied Territories)	500	None
First of October Antifascist Resistance Group (Grupo de Resistencia Anti-Fascista Primero de Octubre) (GRAPO), (Spain)*	Unknown (Est. < 24)	Yes

Great East Islamic Raiders – Front (IBDA-C), (Turkey)	Unknown	None
HAMAS (Islamic Resistance Movement), (Occupied Territories)	Unknown	None
Hizballah (Party of God), a.k.a.: Islamic Jihad, Revolutionary Justice Organization, Organization of the Oppressed on Earth, Islamic Jihad for the Liberation of Palestine, (Lebanon)*	Several hundred	Yes
Irish National Liberation Army (INLA), (Northern Ireland)	< 50	None
Irish Republican Army (IRA), a.k.a.: Provisional Irish Republican Army (PIRA), the Provos, (Northern Ireland)	Several hundred	None
Islamic International Peacekeeping Brigade (IIPB), Chechnya	400	None
Japanese Red Army (JRA), a.k.a.: Anti-Imperialist International Brigade (AIIB), (Lebanon)*	6	Yes
Kahane Chai (Kach), (Israel)	Unknown	None
Kongra-Gel (KGK), a.k.a.: Kurdistan Workers' Party (PKK), a.k.a.: Kurdistan Freedom and Democracy Congress (KADEK), Freedom and Democracy Congress of Kurdistan, (Turkey)	4,000 – 5,000	None
Libyan Islamic Fighting Group, a.k.a.: Al-Jam'a al-Islamiyyah al-Muqatilah, Fighting Islamic Group, Libyan Fighting Group, Libyan Islamic Group, (Libya)	Unknown (Est. several hundred)	None
Lord's Resistance Army (LRA), (Uganda)	Est. 1,000 – 1,500	None
Loyalist Volunteer Force (LVF), (Northern Ireland)	Approx. 300	None
Moroccan Islamic Combatant Group (GICM), (Western Europe)	Unknown	None
New Red Brigades/Communist Combatant Party (BR/PCC), a.k.a.: Brigate Rosse/Partito Comunista Combattente, (Italy)	< 20	None
Orange Volunteers (OV), (Northern Ireland) (Listed in the 2001 State Department Report – Deleted in 2002)	Approx. 20	None
The Palestine Islamic Jihad (PIJ), (Syria)	Unknown	None
Popular Front for the Liberation of Palestine (PFLP), (Syria)*	Unknown	None

Popular Front for the Liberation of Palestine-General Command (PFLP-GC), (Syria)*	Several hundred	None
Qibla and People Against Gangsterism and Drugs (PAGAD), a.k.a.: Muslims Against Global Oppression (MAGO), Muslims Against Illegitimate Leaders (MAIL), (South Africa)*	Unknown (Est. several hundred)	None
Real IRA (RIRA), a.k.a.: True IRA, (Northern Ireland)	100 – 200	None
Red Hand Defenders (RHD), (Northern Ireland)	Approx. 20	None
Revolutionary Nuclei (RN), a.k.a.: Revolutionary Cells, (Greece)*	Unknown (Est. to be small)	Yes
Revolutionary Organization 17 November, a.k.a.: 17November, (Greece)*	Unknown (Est. to be small)	Yes
Revolutionary People's Liberation Party/Front (DHKP/C), a.k.a.: Devrimci Sol, Revolutionary Left, Dev Sol, (Turkey)*	Several dozen	Yes
Revolutionary People's Struggle (ELA), (Greece)*	Unknown	Yes
Revolutionary Proletarian Initiative Nuclei (NIPR), (Italy)*	Approx. 12	Yes
Revolutionary United Front (RUF), (Sierra Leone) (Listed in the 2002 State Department Report – Deleted in 2003)	Est. Several hundred	None
Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs (RSRSBCM), (Chechnya)	$\leq$ 50	None
The Salafist Group for Call and Combat (GSPC), (Algeria)	Unknown (Est. several hundred)	None
Special Purpose Islamic Regiment (SPIR), (Chechnya)	$\leq$ 100	None
The Tunisian Combatant Group (TCG), a.k.a.: Jama'a Combattante Tunisienne, Tunisian Islamic Fighting Group, (Tunisia)*	Unknown	Yes
Turkish Hizballah, (Turkey)	Est. several hundred	None
Ulster Defense Association/Ulster Freedom Fighters (UDA/UFF), (Northern Ireland)	Est. 2,000 – 5,000	None
Ulster Defense Force (UVP), (Northern Ireland)	Unknown (Est. several hundred)	None
Zviadists, (Georgia)	Unknown	None

Table A-5. Terrorist Groups Based in USEUCOM

Other Groups Operating or with Presence in the AOR	
Abu Nidal Organization (ANO)*	*Aum Supreme Truth (Aum)*
Al-Gama'a al-Islamiyya (IG)*	*Mujahedin-e Khalq Organization (MEK)**
Al-Jihad*	*Palestine Liberation Front (PLF)**
Al Qaeda*	

Table A-6. Terrorist Groups with Presence in USEUCOM

U.S. Central Command

Groups Physically Based In AOR	Strength	Anti-U.S. Activity
Abu Nidal Organization (ANO), a.k.a.: Fatah Revolutionary Council, Arab Revolutionary Brigades, Black September, Revolutionary Organization of Socialist Muslims, (Iraq)*	Few hundred	Yes
Al-Badhr Mujahidin (al-Badr), (Pakistan)	Several hundred	None
Al-Gama'a al-Islamiyya (IG), a.k.a.: Islamic Group, (Egypt)*	Unknown	Yes
Al-Ittihad al-Islami (AIAI), a.k.a.: Islamic Union, (Somalia)	2,000 +	None
Al-Jihad, a.k.a.: Egyptian Islamic Jihad, Jihad Group, (Egypt)*	Unknown (Est. several hundred)	Yes
Al –Qaeda, a.k.a.: Qa'idat al-Jihad, (Afghanistan/Pakistan)*	Several thousand	Yes
Ansar al-Islam (AI), a.k.a.: Partisans of Islam, Helpers of Islam, Supporters of Islam, Jund al-Islam, Jaish Ansar al-Sunna, (Iraq)*	Approx. 700 – 1,000	Yes
Harakat ul-Ansar (HUA), (Pakistan)*	Several thousand	Yes
Harakat ul-Jihad-I-Islami (Movement of Islamic Holy War) (HUJI), (Pakistan)	Unknown (Est. several hundred)	None
Harakat ul-Mujahidin (Movement of Holy Warriors) (HUM), a.k.a.: Jamiat ul-Ansar (JUA), (Pakistan)*	Several hundred	Yes
Hizb-I Islami Gulbuddin (HIG), (Afghanistan/Pakistan)*	Several hundred	Yes

Islamic Army of Aden (IAA), a.k.a.: Aden-Abyan Islamic Army (AAIA), (Yemen)*	Unknown	Yes
Islamic Movement of Uzbekistan (IMU), (Uzbekistan)*	< 700	Yes
Jaish-e-Mohammed (Army of Mohammed) (JEM), (Pakistan)	Several hundred	None
Lashkar-e-Tayyiba (Army of the Righteous) (LT), a.k.a.: Jamaat ud-Dawa (JUD), (Pakistan)	Several thousand	None
Lashkar I Jhangvi (Army of Jhangvi) (LJ), (Pakistan)*	< 100	Yes
Mujahedin-e Khalq Organization (MEK or MKO), a.k.a.: National Liberation Army of Iran (NLA), People's Mujahidin of Iran (PMOI), National Council of Resistance (NCR), National Council of Resistance of Iran (NCRI), Muslim Iranian Student's Society, (Iraq)*	Several thousand (3,800 confined to Camp Ashraf)	Yes
Palestine Liberation Front (PLF) (Iraq)*	Unknown	Yes
Sipah-I-Sahaba/Pakistan (SSP), (Pakistan)	Unknown	None

Table A-7. Terrorist Groups Based in USCENTCOM

Other Groups Operating or with Presence in the AOR	
Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya	*Japanese Red Army (JRA)**
Eastern Turkistan Islamic Movement (ETIM)*	*Kurdistan Worker's Party (PKK)*
HAMAS	*Libyan Islamic Fighting Group*
Hizballah*	*Moroccan Islamic Combatant Group (GICM)*
Hizb ul-Mujahidin (HM)	*Palestine Islamic Jihad (PIJ)*
Jamaat ul-Fuqra*	*Popular Front for the Liberation of Palestine-General Command (PFLP-GC)*
Jamiat ul-Mujahidin (JUM)	*The Tunisian Combatant Group (TCG)**

Table A-8. Terrorist Groups with Presence in USCENTCOM

U.S. Pacific Command

Groups Physically Based In AOR	Strength	Anti-U.S. Activity
Abu Sayyaf Group (ASG) (Philippines)*	200 - 500	Yes
Alex Boncayao Brigade (ABB) (Philippines)*	Approx. 500	Yes
Al-Ummah, (India)	Unknown	None
Aum Supreme Truth (Aum), a.k.a.: Aum Shinrikyo, Aleph, (Japan)	< 1,000	None
Cambodian Freedom Fighters (CFF), a.k.a.: Cholana Kangtoap Serei Cheat Kampouchea, (Cambodia)	Unknown (Est. < 100)	None
Chukaku-Ha (Nucleus or Middle Core Faction), (Japan)	3,500	None
The Communist Party of Nepal (Maoist)/United People's Front , (Nepal)*	Several thousand	Yes
Communist Party of the Philippines/New People's Army (CPP/NPA), (Philippines)*	> 10,000	Yes
Eastern Turkistan Islamic Movement (ETIM), (China)*	Unknown	Yes
Harakat ul-Jihad-I-Islami/Bangladesh (Movement of Islamic Holy War) (HUJI-B), (Bangladesh)	> Several thousand	None
Hizb ul-Mujahidin (HM), (India-Kashmir)	Unknown (Est. several hundred)	None
Jamiat ul-Mujahidin (JUM), (India-Kashmir)	Unknown	None
Jemaah Islamiya (JI), (Malaysia and Singapore)*	Unknown (Est. several hundred to several thousand)	Yes
Khmer Rouge/The Party of Democratic Kampuchea, (Cambodia)	100 - 500	None
Kumpulan Mujahidin Malaysia (KMM), (Malaysia)*	Unknown	Yes
Liberation Tigers of Tamil Eelam (LTTE), a.k.a.: World Tamil Association (WTA), World Tamil Movement (WTM), Federation of Associations of Canadian Tamils (FACT), Ellalan Force, Sangilian Force, (Sri Lanka)	Unknown (Est. 8,000 – 10,000)	None
Maoist Communist Center of India (MCCI), a.k.a.: The Maoist Communist Center (MCC) and Naxalites, (India)	30,000	None

Peoples War, a.k.a.: Peoples War Group (PWG) and Naxalites, (India)	Est. 800 – 1,000	None

Table A-9. Terrorist Groups Based in USPACOM

Other Groups Operating or with Presence in the AOR	
Abu Nidal Organization (ANO)*	***Harakat ul-Mujahidin (HUM)****
Al-Badhr Mujahidin (al-Badr)	***Hizballah****
Al-Gama'a al-Islamiyya (IG)*	***Jaish-e-Mohammed (JEM)***
Al Qaeda*	***Japanese Red Army (JRA)****
Harakat ul-Ansar (HUA)*	***Lashkar-e-Tayyiba (LT)***
Harakat ul-Jihad-I-Islami (HUJI)	***Mujahedin-e Khalq Organization (MEK)****

Table A-10. Terrorist Groups with Presence in USPACOM

Groups marked with an asterisk have conducted operations in one or more areas against U.S. targets.

Appendix B
Terrorist Planning Cycle

The main point is to select targets where success is 100% assured.
Dr. George Habash, Founder, PFLP
(Popular Front for the Liberation of Palestine)

Terrorist operations are typically prepared to minimize risk and achieve the highest probability of success. They focus on avoiding the opponents' strengths and concentrating on their weaknesses. Emphasis is on maximizing security and target effects. In practice that means the least number of personnel, and the most effective[233] weapons practicable. To accomplish this, extensive planning is conducted, with an emphasis on target surveillance and reconnaissance.

Collection against potential targets may continue for years before an operation is decided upon. While some targets may be "soft" enough for shorter periods of observation, the information gathering will still be intense. Also, operations planned or underway may be altered, delayed, or cancelled entirely due to changes to the target or local conditions.

Terrorists plan campaigns to combine successive achievements of operational objectives into accomplishing strategic goals. Even though we refer to a terrorist operation having a physical "objective," this physical objective is in reality an intermediate objective. The casualties, destruction, or threats thereof that the operation accomplishes must be properly exploited to reach the target audience. The psychological impact on that audience is the true objective of any terrorist operation. While the assassination of a troublesome police official may provide other tactical advantages, it is the psychological effect on the target audience and its ultimate support of strategic goals that is the true objective. This has been seen extensively in Iraq as terrorists targeted Iraqis serving in provisional Government positions in 2004.

Terrorist Planning Cycle

I — Broad Target Selection

II — Intelligence and Surveillance

III — Specific Target Selection

IV — Pre-attack Surveillance and Planning

V — Attack Rehearsal

VI — Actions on the Objective

VII — Escape and Exploitation
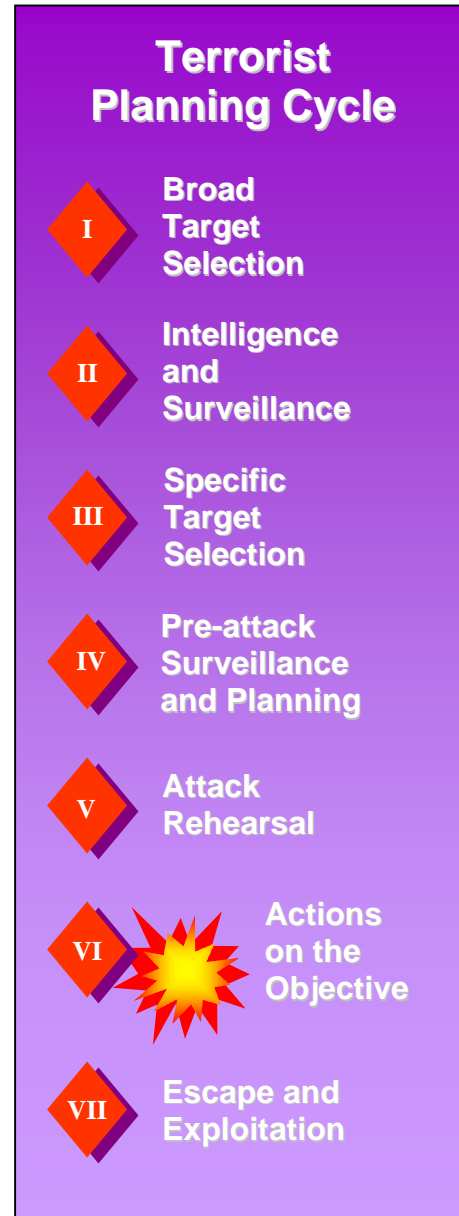
Figure B-1.
Terrorist Planning Cycle

---

[233] Note: "Effective" in this case need not mean modern or destructive, but most suitable to cause the desired target effects. Knives, machetes, and other edged weapons have been extensively used against terrorist victims in the modern era because target audiences view them as particularly bloody and barbarous.

There is no universal "staff school" model for terrorist planning, but experience and success has shown terrorists what works for effective plans and operations. Terrorist organizations exchange personnel and training with each other, and study the methods and operational successes of groups they have no direct contact with. Innovation is a proven key component of operational success. Using new weapons or technology, or old systems in innovative, unexpected ways, allows terrorists to defeat or avoid defensive measures.

Terrorist operational planning can be analyzed according to requirements common to all operations. The planning and operation cycle below is valid for traditional hierarchically organized groups, as well as the decentralized "network" type organizations. The differences between the two organizations are the location of decision making at the various steps of the cycle, and the method of task organizing and providing support for the operation.

Phase I: Broad Target Selection

> **"Information gathering is a continuous operation…"**
>
> Irish Republican Army's *Handbook*
> *for Volunteers of Irish Republican Army,* 1956.

This phase is the collection of information on a large number of potential targets, some of which may never be attacked, or seriously considered for attack. Personnel that are not core members of the terrorist organization, but are either sympathizers or dupes, and who may not be aware of what their information will be used for, often conduct this data collection. This phase also includes open source and general information collection. Some features of this type of collection are:

- Stories from newspapers, other media, and journalistic sources often provide key information on the target.

- Internet research provides texts, pictures, blue prints, and video information.

- Potential targets are screened based on symbolic value and their potential to generate high profile media attention. Objectives of the terrorist group influence the selection of a person or facility as a worthy target. This includes the likely casualty rate achieved by the attack.

The number of preliminary targets that can be screened is limited only by the capabilities of the group to collect information from sympathizers and open sources. Targets that are considered vulnerable and which would further the terrorist organization's goals are selected for the next phase of intelligence collection.

Phase II: Intelligence Gathering and Surveillance

Targets showing potential vulnerabilities are given a higher priority of effort. This priority establishes the requirement to gather additional information on the targets' patterns over time. Examples include the 2004 accounts of terrorist surveillance conducted for years on the International Monetary Fund, Prudential Building, New York Stock Exchange, as well as facilities in Las Vegas, Nevada. The type of surveillance employed depends on the target type. Elements of information typically gathered include:

- Practices/Procedures/Routines – For facilities this includes scheduled deliveries, work shift changes, identification procedures and other observable routines. For individuals, it can include regularly scheduled errands (laundry pick up every third day, etc.) and appointments.

- Residence & Workplace – This category applies primarily to the physical layout and individual activities at the two places the target typically spends the most time.

- Transportation/Routes of Travel – For individuals, this is the mode of transport and common routes to any regular destination (house, work, gym, school, etc.). For facilities, it addresses ingress and egress points, types of vehicles allowed on the grounds, or availability of transportation into the target site.

- Security Measures – This topic includes a myriad of potential collection areas, depending on the complexity of the security around the target. Presence of a guard force; the reaction time of response units; any hardening of structures, barriers, or sensors; personnel, package, and vehicle screening procedures; and the type and frequency of emergency reaction drills are examples of key collection objectives. This is one of the most important areas of information for attack site selection, since the intent is to bypass and avoid security measures, and be able to strike the target during any period.

Phase III: Specific Target Selection

Selection of a target for actual operational planning considers some of the following factors:

- Does success affect a larger audience than the immediate victim(s)?

- Will the target attract high profile media attention?

- Does success make the desired statement to the correct target audience(s)?

- Is the effect consistent with objectives of the group?

- Does the target provide an advantage to the group by demonstrating its capabilities?

- What are the costs versus benefits of conducting the operation?

A decision to proceed requires continued intelligence collection against the chosen target. Targets not receiving immediate consideration will still be collected against for future opportunities.

Phase IV: Pre-attack Surveillance and Planning

Members of the actual operational cells begin to appear during this phase. Either trained intelligence and surveillance personnel, or members of the cell organized to conduct the operation conduct this phase. Consequently, the level of intelligence tradecraft and operational competency correspondingly increases. This phase gathers information on the target's current patterns over time, usually days to weeks. It allows the attack team to confirm the information gathered from previous surveillance and reconnaissance activities. The areas of concern are essentially the same as in Phase II, but with greater focus based upon the planning conducted thus far.

The type of surveillance employed depends on the target's activities. The information gained is then used to:

- Conduct security studies.

- Conduct detailed preparatory operations.

- Recruit specialized operatives (if needed).

- Procure a base of operations in the target area (safe houses, caches, etc.).

- Design and test escape routes.

- Decide on type of weapon or attack.

Phase V: Rehearsals

As with conventional military operations, rehearsals are conducted to improve the odds of success, confirm planning assumptions, and develop contingencies. Terrorists also rehearse to test security reactions to particular attack profiles. Terrorists use both their own operatives and unwitting people to test target reactions.

Typical rehearsals include:

- Deployment into target area.

- Actions on the objective.

- Escape routes.

- Equipment and weapon performance.

Tests in the target area will be conducted to confirm:

- Target information gathered to date.

- Target pattern of activities.

- Physical layout of target or operation area.

- Security force reactions (state of alert, timing, size of response, equipment, routes).

Phase VI: Actions on the Objective

Once terrorists reach this stage of their program, the odds are clearly against the target. Several different analyses conclude that once operations are initiated, the success rate for the terrorist is in the ninety-percent range. Terrorists will minimize time spent conducting the actual operation to reduce their vulnerability to discovery or countermeasures. With the exception of barricade-style hostage taking operations, terrorists plan to complete their actions before even nearby security forces can react.

Terrorists conducting planned operations possess important tactical advantages. Since they are the attacker, they possess all the advantages of initiative, giving them:

- Surprise.

- Choice of time, place, and conditions of attack.

- Employment of diversions and secondary or follow-up attacks.

- Employment of security and support positions to neutralize target reaction forces and security measures.

Because of the extensive preparation through surveillance and reconnaissance, enemy security measures will be planned for and neutralized. Any countermeasure can be countered in turn. If security cameras are detected, they can be avoided or disabled as necessary. Guards can be overcome or killed. Hardened vehicles or buildings will result in the use of larger or more effective explosive devices or direct fire weapons. Although security measures may complicate the attackers' problems, they do not confer any guarantee against attack.

Phase VII: Escape and Exploitation

Escape plans are usually well rehearsed and executed. Many terrorists want to survive the operation and escape. It further enhances the effect of fear and terror from a successful operation if the perpetrators get away "clean." The exception to this is a suicide operation, where the impact is enhanced by the willingness to die in achieving the attack. Even in suicide attacks, however, there are usually support personnel and "handlers" who must deliver the suicide asset to the target, and subsequently make their escape.

Exploitation is the primary objective of the operation. The operation must be properly exploited and publicized to achieve its intended effect. Media control measures, prepared statements, and a host of other preparations are made to effectively exploit a successful operation. These will be timed to take advantage of media cycles for the selected target audiences.

Unsuccessful operations are disavowed when possible. The perception that a group has failed severely damages the organization's prestige and makes it appear vulnerable, or worse, ineffective. Once a terrorist organization is perceived as ineffective, it is very difficult to impact target audiences.

In addition to the impact on the opponent, successful attacks bring favorable attention, notoriety and support (money, recruits, etc.) to the group conducting them. If the group conducting the operation subscribes to a revolutionary ideology, they will see each success as gradually inspiring more revolutionary fervor in the population. Any success encourages the terrorists to conduct further operations, and improves their ability to do so through increased support and experience.

**Appendix C
Terrorist Operations and Tactics**

Not believing in force is the same as not believing in gravity.

Leon Trotsky

Terrorist Operations

The discussion below presents the most common types of terrorist operations and tactics. By no means is this intended to be an exhaustive discussion of this topic since the combination of methods and approaches is virtually unlimited. However, one constant regarding terror operations is the use of techniques stressing surprise, secrecy, innovation, and indirect methods of attack. Their tactics are as broad and diverse as the imagination of the group's members. Additionally, with the use of the Internet and common training bases, terrorist groups exchange information on tactics that yield success. Al Qaeda alone has assembled in excess of 10,000 pages of written training material, more than a hundred hours of training videos, and operates a worldwide network of training camps.[234] Additionally, they have been able to field test their tactics in real-world situations since many of the terrorists have participated in conflicts such as Chechnya, Kashmir, Afghanistan, the Balkans, and Iraq.

For military professionals, a key principle to keep in mind is the difference in outlook between terror operations and military operations. The terrorist will utilize tactics, forces, and weapons specifically tailored to the particular mission. Terrorist operations are individualistic, in that each is planned for a specific target and effect. Additionally, terrorists will only expose as much of their resources and personnel to capture or destruction as are absolutely necessary for mission accomplishment. A military force would approach an operation with plans to

Figure C-1: **Khobar Towers** (*Source*: DOD Photo)

concentrate forces and keep excess combat power on hand to meet contingencies, ensure mission success, and prepare for follow-on missions. A terrorist takes a minimal force and relies upon prior planning and reconnaissance to match the force, weapons, and methods to

---

[234] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat, An Analytical Guide to al-Qaeda's Tactics & Targets* (Alexandria: Tempest Publishing, 2003), 7.

the target. There is no concept of "follow-on missions", so there is no need for redundant capability. If changes to the target, or unexpected conditions render success unlikely, he will usually cancel the operation and return later with a better weapon, an updated plan, more personnel, or whatever it may require to ensure a successful operation. For major terrorist operations, mission accomplishment will in all likelihood mean the disbanding of the force, personnel returning to their cells and covers, or forming new task groups for other operations.

In addition to adaptive and flexible organizations, terrorists also employ specific equipment built or procured for a particular operation. Because of the lag time between development of a new technology and military acquisition and fielding, terrorists can sometimes procure equipment superior to standardized military models. As an example, instead of purchasing hundreds of identical radios constructed to meet all likely uses, a terrorist will only procure the quantity he needs of the newest, most capable radio appropriate for the operation. The only real limitation is funding and availability of the equipment when it is needed.

Weapons will also be tailored to the particular operation. If a directional explosive is needed, the terrorist could make use of available military models of anti-tank and anti-personnel mines. Conversely, the terrorist may determine that a mine would be detected by the target's security force en route to the attack, and he therefore needs to build or obtain an alternative device. To illustrate, even counting the warheads of anti-ship cruise missiles, there was not a readily available weapon for the attack on the USS *Cole*. No one manufactures a half-ton C-4 platter charge configured to fit in a small boat,[235] but that was exactly what the terrorist's plan required. Therefore it was exactly what the terrorist group built. Additionally, Operation Iraqi Freedom has demonstrated the terrorists' ability to construct a variety of IEDs that are effective, yet are easily emplaced and difficult to detect by military forces.

Objectives of the group(s) conducting the operation are key to predicting likely targets. Is the intent to cause loss of faith in the authorities, a provocation to inspire resistance, to promote fear amongst the population, or to inflict military casualties in an attempt to reduce national and political will? Although several different types of operations may satisfy a particular objective, terror groups often develop expertise in one or more types of operations, and less specialization in others.

Some groups will actually publish their targeting guidance. In March 2004, al Qaeda published a 9-page article in their training publication, "Camp al-Battar Magazine" that released new targeting guidance to its members and other affiliated groups. This publication contains information on everything from small arms skills, physical fitness, targeting, tactics, and secure communications. The new guidance specifically covered targets within cities, addressing faith targets, economic targets, and human targets.[236]

Assassination

An assassination is a deliberate action to kill specific individuals, usually VIPs (political leaders, notable citizens, collaborators, particularly effective officials, etc.), versus the killing

---

[235] John McWethy et al., no title, *ABCNews.Com,* 18 October 2000; available from http://www.abcnews.go.com/sections/world/ DailyNews/cole001018b.html; Internet; accessed 9 January 2003.
[236] Ben N. Venzke, *al Qaeda Targeting Guidance* - Version 1.0 (Alexandria, VA: IntelCenter/Tempest Publishing, LLC, 2004), 3-5.

of common people, which is considered murder. The terrorist group assassinates or murders people it cannot intimidate, people who have left the group, people who support the "enemy," or people who have some symbolic significance for the enemy or world community. Terrorist groups often refer to these killings as "punishment" or "justice" as a way of legitimizing them. In 1981, President Anwar Sadat of Egypt was assassinated by fundamentalist Islamics for his support of peace in the Middle East and his relationship with the West. In September 2001, Northern Alliance leader Ahmed Shah Massoud was assassinated in Afghanistan by two suicide bombers, believed to be from al Qaeda, due to his opposition to the Taliban regime and al Qaeda's presence in Afghanistan.

Many targets of assassination are symbolic and are intended to have great psychological impact on the enemy. For example, assassinating an enemy government official, a successful businessperson, or a prominent cleric can demonstrate the enemy's inability to protect its own people. Assassinating local representatives of social or civic order, such as teachers, contributes to disorder while demoralizing other members of the local government and discouraging cooperation with them. An excellent example of this is the attempted assassination of Iraq's most prominent Shiite cleric, Grand Ayatollah Ali al-Sistani in February 2004. This incident was an apparent attempt to create anger in the long oppressed Shiite community and increase the sectarian and ethnic tensions in post-war Iraq. There have also been a number of assassinations of Iraqis who have assumed leadership positions in support of a transition to a democratic government.

Printed training materials and videos from al Qaeda provide guidance on various methods to conduct assassinations, and also details the critical parts of the body to target with each method. [237] Assassination methods include remotely detonated bombing, the use of firearms, knives, heavy weaponry such as anti-tank rocket launchers, and poisoning. However, bombings and shootings are the most common methods.

Extensive target surveillance and reconnaissance of engagement areas are required to select the optimum mode of attack. Although many factors play into the decision, the target's vulnerabilities ultimately determine the method of assassination. For example, a target driving to work along the same route each day may be vulnerable to an emplaced explosive device.[238] Such action requires detailed planning, similar to that for a kidnapping. The main difference is that a kidnapping seeks to keep the target alive (at least, initially), while an assassination or murder does not.

Two notable assassination attempts directed against the American military were conducted by the Red Army Faction in Europe. In 1979, they attempted to kill General Alexander Haig when he was the SACEUR using an explosive device planted on his preferred route to the office. The second attempt was against General Frederick Kroesen in 1981 when he was the CINC, USAEUR using small arms and a rocket launcher against his motorcade. In both cases, the terrorists had conducted surveillance and developed detailed plans for the assassination attempts. However, both attempts fortunately failed. In the case of General Haig, his vehicle was traveling faster than expected and the blast barely impacted the rear of

---

[237] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat, An Analytical Guide to al-Qaeda's Tactics & Targets* (Alexandria: Tempest Publishing, 2003), 14.
[238] *Encyclopedia of World Terror*, 1997 ed., s.v. "Assassination."

his car. In the attack on General Kroesen, the armor and bulletproof glass on his vehicle, combined with an inaccurate rocket detonation, prevented any serious injuries.

Unfortunately terrorists have been successful in some assassination attempts. In April 1989, Communist insurgents from the New People's Army in the Philippines assassinated an American military advisor, Col. James Rowe. He was killed in a moving ambush where small arms fire defeated the protection of his armored official vehicle. This group, which is a DFTO based in the Philippines, was attacking Americans they considered directly linked to the Philippine military campaign being conducted against their group.

Hostage Taking and Barricade Situations

Hostage taking is typically an overt seizure of people to gain publicity for a cause, gain political concessions, political asylum, release of prisoners, or ransom. Many times the terrorists will take hostages with the intent to kill them after they believe they have fully exploited the media coverage from the situation.

Unlike kidnapping where a prominent individual is normally taken and moved to an unknown location, the hostages are usually not well known figures in the enemy's society. While dramatic, hostage situations are frequently risky for the terrorist group, especially when conducted in enemy territory. They expose the terrorists to hostile military or police operations, and carry significant possibility of both mission failure and capture. Therefore, terrorists will usually attempt to hold hostages in a neutral or friendly area, rather than in enemy territory. Since hostage taking is risky, the benefits must warrant conducting this type operation. For example, if the enemy captures the leader or principal members of the terrorist group, the group may take hostages to exchange for its key personnel.

An excellent example of a hostage situation was the Moscow theater siege in October 2002. Thirty-four Chechen terrorists seized a movie theater, threatening to kill all of the hostages if the Russians did not meet their demands. The rebels were demanding that Russian forces end the war in the breakaway republic of Chechnya. Following a long stalemate, Russian forces assaulted the theater. Sixty-seven hostages died as well as the 34 terrorists. However, 750 hostages were released.

Another example is the hijacking of TWA Flight 847 from Athens to Rome in 1985 by two members of Hizballah. They held the plane and 153 hostages for 17 days demanding the release of Lebanese and Palestinian prisoners. The hostages were released after Israel freed 435 prisoners. However, a U.S. Navy diver, Robert Stethem, was killed and his body was dumped on the tarmac during the ordeal.

Kidnapping

Kidnapping is usually an action taken against a prominent enemy individual for a specific reason. The most common reasons for kidnapping are ransom, release of a fellow terrorist, or the desire to publicize a demand or an issue. The terrorist group conducts detailed planning, especially regarding movement of the kidnapped individual. The risk in kidnapping is relatively lower than in hostage taking primarily because the kidnapped victim is moved to a

location controlled by the group. The group makes demands and is willing to hold a victim for a significant time, if necessary.

The success of kidnapping relies upon balancing the cost to the government represented by the threat of harm to the victim, with the costs of meeting the kidnappers' demands. Some kidnapping operations are actually assassinations, as the death of the victim is intended from the start. The terrorists intended objective in this case being the intermediate concessions and publicity obtained during the negotiation process that they would not receive from a simple assassination.

Kidnapping (and hostage taking) can also be used as a means of financing the organization. Ransom from seized individuals or groups are a significant slice of income for groups in several regions of the world. Latin America has long been a victim of terrorist kidnapping, especially by the FARC and ELN in Colombia. The Abu Sayyaf Group in the Philippines also uses this method to finance their operations. Although the sizes of the ransoms vary, they often can be quite large. Ten employees of a Spanish energy consortium were kidnapped in Ecuador in October 2000 by kidnappers believed to be linked to the Popular Liberation Army of Colombia. The oil companies eventually paid $13 million in ransom for their release.

An example of the U.S. military's experience with kidnapping is the case of USMC Col. William (Rich) Higgins. He disappeared on May 17, 1988, while serving as the Chief, Observer Group Lebanon and Senior Military Observer, United States Military Observer Group, United Nations Truce Supervision Organization. He was kidnapped and held by Iranian-backed Hizballah terrorists and later murdered. A picture of his body hanging from a noose was released to the news media in July 1989. His remains continued to be held until they were released in December 1991.

Another example was the kidnapping of Brigadier General James Dozier, senior American official at a NATO headquarters in Verona, Italy, by Red Brigade terrorists on December 17, 1981. The targeting of General Dozier broke the pattern of previous terrorist activities in Italy since terrorist groups had previously concentrated their actions against key Italian personalities, such as senior Italian politicians, industrialists, jurists, newspaper publishers and police officials. Following General Dozier's kidnapping, numerous additional threats were received which provided a clear indication that the situation had changed in Italy and other Americans and U.S. facilities were potential targets for terrorist actions.[239]

The terrorists conducted surveillance of General Dozier's residence for at least 30 days from positions in a park and at a bus stop across from the building. The techniques used were young people standing at the bus stop and young couples in the park area. Additionally, the terrorists had been in his apartment at least twice while posing as meter readers. Two men pretending to be plumbers conducted the actual kidnapping. They told General Dozier that there was a leak in the apartment below and wanted to determine if it was coming from Dozier's apartment. Since leaks were common in the building, he let them into the apartment,

---

[239] COL Thomas D. Phillips, "The Dozier Kidnapping: Confronting the Red Brigades," Air and Space Power Chronicles (February 2002): 1; available from
http://www.airpower.maxwell.af.mil/airchronicles/cc/phillips.html; Internet; accessed 31 March 2004.

at which time the kidnapping was executed. After being held for 42 days, he was rescued by Italian police.[240]

Kidnapping and periodic murder of victims is a recurring technique of terrorists. A number of recent civilian and military member kidnappings and murders in the Middle East received significant international media coverage. As noted in Chapter 4, these types of acts appear to be an increasing method of terrorism.

Raid

A terrorist raid is similar in concept to a conventional operation, but is usually conducted with smaller forces against targets marked for destruction, hijacking, or hostage/barricade operations. In these cases, the raid permits control of the target for the execution of some other action. The kidnapping or assassination of a target that has a security force can often require a raid to overcome the defenses. Successful execution of these type attacks requires extensive preoperational surveillance and detailed planning.

Examples of this type tactic are the raids conducted by terrorists on three Riyadh western housing compounds in Saudi Arabia on 11 May 2003. Attackers penetrated each compound and then detonated vehicle borne IEDs. The attack at the al-Hamra compound demonstrates the tactics used in a raid such as this. A Toyota sedan pulled up to the gate, followed by a GMC Suburban. A number of terrorists then dismounted, shot the guard, and then forced their way into the compound. As both vehicles drove to the center of the compound, terrorists shot into buildings and at any moving targets. Once they reached the housing area, a suicide terrorist detonated the explosive device in the GMC Suburban.[241]

Extortion

Extortion is the act of obtaining money, materiel, information, or support by force or intimidation. Extortion is often used during the formative period of a group or by groups that fail to develop more sophisticated financial skills. However, the opportunity to engage in more lucrative money making activities, such as drug trafficking, may eventually replace the need to extort by some groups. Extortion takes the form of "war taxes" or protection money. Depending on the structure of the terrorist organization, the logistics and support cells extort money from local businesses in exchange for protection, which means not harming or bothering the business or its members. Members of the intelligence cells may also extort to collect required information.

The Basque terrorists are an excellent example of a group that uses extortion. They have extorted money for years from businesses to finance their battle for independence. When Spain converted from the peseta to the euro, ETA even sent letters to Basque businesses demanding payments ranging from 30,000 to 60,000 euros. Although many of the large

---

[240] U.S. Marine Corps, Marine Corps University, Corporals Noncommissioned Officers Program, Force Protection, Course CPL 0302, (Quantico, VA, January 1999), 12-13; available from http://www.tecom.usmc.mil/utm/Force_Protection1_LP.PDF; Internet; accessed 31 March 2004.
[241] Department of State, U.S. Embassy, Jakarta, Indonesia, *Threats Involving Vehicle Borne Improvised Explosive Devices* (Jakarta, Indonesia, 2003), 2; available from http://www.usembassyjakarta.org/vbied_vehicles.html; Internet; accessed 14 January 2004.

companies in the Basque region refuse to pay ETA's "revolutionary tax", smaller businesses that cannot afford to hire bodyguards are forced to pay.[242]

Another form of extortion is intimidation. Intelligence cells or a specialized team intimidates people to obtain information on the group's enemy or to provide resources. Death threats against an individual or his family cause him to provide information or resources to a group with which he has no interest. A terrorist group also intimidates people not to take action. For example, enemy security personnel may not implement required security measures because of intimidation. The information cell of a terrorist group helps create and maintain the fear caused by extortion through its propaganda and deception actions.

The power of extortion and blackmail as a means of coercing individuals should not be underestimated. Several terrorist groups have successfully used these techniques to force individuals to carry out suicide bombing missions.

Ambush

An ambush is a surprise attack characterized by violence of execution and speed of action. Terrorists' use of this tactic is similar in concept to conventional military operations. The intended objective may be to cause mass casualties, assassinate an individual, or disrupt hostile security operations. Explosives, such as bombs and directional mines, are a common weapon used in terrorist ambushes. They are powerful and can be remotely detonated. Other weapons frequently used are rocket launchers, automatic weapons, and pistols.

The varieties of firepower and ambush tactics used by terrorists have been repeatedly demonstrated in Iraq during recent years as coalition forces and civilians are attacked. However, this is a common tactic used by terrorist groups around the world. As discussed earlier in this appendix, terrorists in Europe ambushed the motorcades of both General Haig and General Kroesen. However, terrorists do not limit their targets to just prominent individuals. In the Balkans in August 2001, Albanian terrorists ambushed a Macedonian security force convoy using mortars and rocket launchers killing 10 members of the security force.

Terrorist ambushes are frequently conducted from a variety of mobile platforms. Cars, vans and motorcycles have been used to conceal the attackers, isolate or immobilize the target, and then allow the attackers to escape. Ambushes from mobile platforms can be conducted while moving, or can be designed to bring the target to a halt in order to allow the attack team to physically close with and destroy the target. The 1989 assassination of Colonel Rowe in the Philippines described earlier is an example of a mobile ambush, as is the more recent March 2004 attack on five U.S. civilians working for a private volunteer organization (PVO) in Iraq. Four were killed and one was wounded in this mobile ambush in the city of Mosul.

Hijacking

Hijacking involves the forceful commandeering of a conveyance. Although normally associated with planes, it can also include naval vessels or other craft. There are many purposes to hijacking, such as hostage taking activities, procuring a means of escape, or as a

---

[242] "Terrorists Demand Extortion Cash in Euros," *TCM Breaking News* (4 September 2001): 1; available from http://archives.tcm.ie/breakingnews/2001/09/04/story22584.asp; Internet; accessed 31 March 2004.

means of destruction. While hijacking of aircraft for hostage taking has declined in frequency since the implementation of improved security measures, the use of hijacked aircraft for escape or as destructive devices continues and terrorist groups have a significant amount of information on how to conduct hijacking operations. The attacks on the World Trade Center and the Pentagon in September 2001 are vivid reminders of the hijacking abilities of terrorist groups and the destructive power of hijacked airliners.

The use of hijacked vehicles for destructive devices is not restricted to aircraft. Trucks carrying cargoes of explosive or flammable materials have also been seized to use as delivery devices. The possibility of such a technique being used with a ship carrying oil, refined petroleum products, or liquefied natural gas (LNG) is of great concern. The horrific results of several accidental explosions and fires from mishaps in handling such vessels in port show the catastrophic potential of this technique.[243] Ships exploding in the harbors of Texas City, Texas in 1947 and Halifax, Nova Scotia in 1917 destroyed significant portions of these towns, and had a combined death toll of over 2500.

Sabotage

Sabotage is the planned destruction of the enemy's equipment or infrastructure. The purpose of sabotage is to inflict both psychological and physical damage. This can result from an incident creating a large number of casualties or from a severe disruption of services for the population. Sabotage demonstrates how vulnerable the enemy is to the terrorist group's actions. Destroying or disrupting key services or facilities impresses the power of the saboteur on the public consciousness, and either increases their frustration with the ineffectiveness of the government, or inspires others to resist.

A terrorist group normally aims its sabotage actions at elements of infrastructure, in order to reinforce the perception that nothing is safe. The action can have significant economic impacts, as well as the additional effects of creating mass casualties. Oil pipelines, water purification plants, sewage treatment facilities, air traffic control hubs, and medical treatment or research facilities are just a few examples of potential targets. Terrorist groups use many techniques, such as bombing, arson, cyber, or use of contaminates, to conduct sabotage.

Examples of sabotage have been evident in Iraq since the end of major combat operations where attacks have been conducted against power generation facilities and water pipelines. Additionally, attacks on Iraq's oil pipeline have been persistent and estimates in September 2003 were that the country was losing $7 million daily because of damage to the pipeline that carried oil from the Kirkuk fields to a Mediterranean port in Turkey.[244]

Aircraft Attacks

A significant concern is the attempt by terrorists to shoot down aircraft using some form of manportable air defense system (MANPADS) or improvising other systems for this use. There are a number of weapons that terrorists can use to down aircraft and they have demonstrated in the past that they can be successful.

---

[243] Gerald Pawle, *Secret Weapons of World War II* (New York: Ballantine Books, 1967), 53-54.
[244] "Saboteurs Disable Critical Iraqi Oil Pipeline," *HoustonChronicle.com*, 8 September 2003; available from http://www.chron.com/cs/CDA/ssistory.mpl/special/iraq/2087438; Internet; accessed 16 January 2004.

Although part of military operations, probably the most notable incident by terrorists/insurgents downing U.S. military aircraft was in Mogadishu, Somalia in 1993. In compliance with United Nations Security Resolution 814, the United States was conducting a raid to capture some of the close supporters of the leader of one of the rival Somali clans, General Mohammed Farah Aideed. During this raid, two UH-60 Blackhawk helicopters were shot down using RPGs. The U.S. had underestimated Aideed's ability to shoot down its helicopters using this type system. However, he had brought in fundamentalist Islamic soldiers from Sudan, who had experience shooting down Russian helicopters in Afghanistan, to train his men to use RPGs in an air defense role.[245] Once again, U.S. military forces realized the threat posed by RPGs in an air defense mission in Afghanistan in 2002 when two MH-47 Chinook helicopters were brought down in the Shah-e-Kot area by this same system.

The main concern from terrorists; however, is use of shoulder-fired surface-to-air missiles, also known as MANPADs. These systems normally contain an infrared (IR) seeker with the missile providing little opportunity for warning before impact on the target. The Afghan mujahedeen demonstrated MANPADs lethality by destroying 269 Soviet aircraft during the Soviet Union's war in Afghanistan. Additionally, 56% of the kills and 79% of the Allied aircraft damaged during Desert Storm were through these weapons.[246]

These missiles are very affordable by terrorist groups, and they are widely available on the world weapons market. Unclassified estimates range from 5,000 to 150,000 shoulder-fired SAMs are in terrorist hands. Although the range of these estimates varies considerably, it does demonstrate the concern over the proliferation of these type systems. To demonstrate the number of systems in circulation, as of December 2002, coalition forces in Afghanistan had captured over 5,500 shoulder-fired systems from the Taliban and al Qaeda. Some of these included U.S. Stinger and British Blowpipe missiles.[247]

Although these weapons have a target engagement range of a few miles, most experts consider aircraft departures and landings as the times when aircraft are most vulnerable to these weapons. Over the past 25 years, 35 civilian aircraft have come under attack from these weapons, resulting in 24 aircraft being shot down and more than 500 deaths. Of these encounters; however, only 5 incidents involved large airliners. [248] (See Table C-1).

---

[245] FM 3-06, *Urban Operations*, 1 June 2003.

[246] "Man Portable Air Defense System (MANPADS)," *Global Security.org* (n.d.): 1; available from http://www.globalsecurity.org/military/intro/manpads.htm; Internet; accessed 19 March 2004.

[247] Christopher Bolkcom, et al, *Homeland Security: Protecting Airliners from Terrorist Missiles* (Washington, D.C.: Congressional Research Service Report for Congress, 3 November 2003), 4-7; available from http://www.fas.org/irp/crs/RL31741.pdf; Internet; accessed 1 April 2004.

[248] Ibid., 7-9.

Date	Location	Aircraft	Operator	Outcome
8 Nov 1983	Angola	Boeing 737	Angolan Airlines (TAAG)	Catastrophic: 130 fatalities of 130 people on board.
9 Feb 1984	Angola	Boeing 737	Angolan Airlines (TAAG)	Hull Loss: aircraft overran runway on landing after being struck by a missile at 8,000 feet during climbout. No fatalities with 130 on board.
21 Sep 1984	Afghanistan	DC-10	Ariana Afghan Airlines	Substantial Damage: aircraft was damaged by the missile, including damage to two hydraulic systems, but landed without further damage. No fatalities.
10 Oct 1998	Democratic Republic of Congo	Boeing 727	Congo Airlines	Catastrophic: 41 fatalities of 41 people on board.
19 Nov 2002	Kenya	Boeing 767	Arkia Israeli Airlines	Miss: two SA-7's were fired at the aircraft during climbout, but missed. No fatalities.

Table C-1: Large Civilian Turbojet Aircraft Encounters with Shoulder-Fired Missiles (1978-Present)

Unclassified estimates reflect between 25 and 30 non-state groups possess these MANPADS systems. The table below depicts the groups that are believed to be in possession of these weapons through the time period 1996 – 2001.[249]

Group	Location	Missile Type
Armed Islamic Group (GIA)	Algeria	Stinger (c)
Chechen Rebels	Chechnya, Russia	SA-7 (c), Stinger (c), Blowpipe (r)
Democratic Republic of the Congo (DRC) Rebel Forces	Democratic Republic of the Congo	SA-16 (r)
Harkat ul-Ansar (HUA)	Kashmir	SA-7 (c)
Hezbullah	Lebanon	SA-7 (c), QW-1 (r), Stinger (r)
Hizbul Mujahideen (HM)	Kashmir	Stinger (r)
Hutu Militiamen	Rwanda	Unspecified type (r)
Jamaat e Islami	Afghanistan	SA-7 (c), SA-14 (c)
Jumbish-i-Milli	Afghanistan	SA-7 (c)
Khmer Rouge	Thailand/Cambodia	Unspecified type (r)
Kosovo Liberation Army (KLA)	Kosovo	SA-7 (r)
Kurdistan Workers Party (PKK)	Turkey	SA-7 (c), Stinger (c)
Liberation Tigers of Tamil Eeelam (LTTE)	Sri Lanka	SA-7 (r), SA-14 (r), Stinger (c), HN-5 (c)

---

[249] Ibid., 5-6.

Oromo Liberation Front (OLF)	Ethiopia	Unspecified type (r)
Palestinian Authority (PA)	Palestinian autonomous areas and Lebanon	SA-7 (r), Stinger (r)
Popular Front for the Liberation of Palestine – General Command (PFLP-GC)	Palestinian autonomous areas and Lebanon	Unspecified type (r)
Provisional Irish Republican Army (PIRA)	Northern Ireland	SA-7 (c)
Revolutionary Armed Forces of Colombia (FARC)	Colombia	SA-7 (r), SA-4 (r), SA-16 (r), Redeye (r), Stinger (r)
Rwanda Patriotic Front (RPF)	Rwanda	SA-7 (r), SA-16 (r)
Somali National Alliance (SNA)	Somalia	Unspecified types (r)
Al Qaeda/Taliban	Afghanistan	SA-series (c), Stinger (c), Blowpipe (c)
National Liberation Army (ELN)	Colombia	Stinger (r), Unspecified types (r)
National Liberation Army (UCK)	Macedonia	SA-18 (c)
National Union for the Total Independence of Angola (UNITA)	Angola	SA-7 (c), SA-14 (r), SA-16 (r), Stinger (c)
United State WA Army	Myanmar	SA-7 (c), HN-5N (c)
United Somali Congress – Somali Salvation Alliance (USC-SSA)	Somalia	Unspecified types (r)
Note: (c) is possession confirmed through intelligence sources or actual events; (r) is reported but not confirmed.		

Table C-2: Non-State Groups with Shoulder-Fired SAMS (1996-2001)

Maritime Operations

Terrorist attacks against maritime targets are fairly rare and constitute only 2% of all international incidents over the last 30 years.[250] However, there is a history of maritime terrorism and maritime authorities worldwide are increasingly anxious about terrorist attacks on both ports and ships. In fact, some intelligence analysts believe that because land-based targets are better protected, terrorists will turn to the maritime infrastructure because they see these as "softer" targets.[251]

Likely operations conducted by maritime terrorism include suicide attacks on commercial and military vessels, and hijacking for the following purposes: (1) carrying out a subsequent suicide attack on a ship or port (2) seeking ransom (3) smuggling weapons and explosives (4) simple piracy.[252]

Although few terrorist groups have developed a maritime capability, there have been some exceptions, to include the Provisional Irish Republican Army, Abu Sayyaf Group based in the Philippines, various Palestinian groups, al Qaeda, and the Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka. In fact the LTTE has quite a large maritime capability to include both coastal and deep-water craft and they have developed a reputation of being the best in the world in this arena.[253] They reportedly have roughly 3000 trained personnel and between 100-200 surface and underwater vessels, including attack

---

[250] Peter Chalk, "Threats to the Maritime Environment: Piracy and Terrorism," (RAND Stakeholder Consultation, Ispra, Italy 28-30 October 2002): 9.

[251] Graham Gerard Ong, "Next Stop, Maritime Terrorism," *Viewpoints* (12 September 2003): 1; available from http://www.iseas.edu.sg/viewpoint/ggosep03.pdf; Internet; accessed 2 April 2004.

[252] Ibid., 2.

[253] Ibid., 1.

vessels, logistics vessels, fast personnel carriers, suicide craft, and multi-purpose craft. Additionally, they have employed a range of technologies, including suicide stealth craft, mini submarines, and one-man suicide torpedoes.[254]

Information presented at the Terrorism in the Asia Pacific Conference in September 2002 reported that al Qaeda had obtained a variety of vessels and systems capable of carrying out attacks against ships and seaports. These included mini-subs, human torpedo systems, and divers trained in underwater demolitions. The larger vessels are commercial ships that are used to generate revenue for al Qaeda. However, there is concern that they could be filled with explosives and used as floating bombs to ram into other ships or port facilities.[255]

The International Maritime Organization has warned that liquefied natural gas (LNG) carriers and other ships carrying volatile cargo could be hijacked and used as weapons of mass destruction. In fact a briefing at the Maritime Security Council's annual International Maritime Security Summit in October 2002 stated that a large ship loaded with LNG could result in an explosion equivalent to a .7-megaton nuclear detonation. (The bomb dropped on Hiroshima, Japan was 15-kilotons.)[256] The damage this could create if it occurred in a port, such as the Norfolk Naval Base, would be quite substantial.

The best-known maritime terrorist attack against the U.S. military is the attack on the USS *Cole*, which occurred in October 2000. Two suicide bombers in a small explosive laden boat with a platter charge attacked the ship while it was refueling in Aden Harbor, Yemen. The blast, which blew a 40 by 60-foot hole in the side of the USS *Cole*, killed 17 and injured 39 U.S. crewmen. The al Qaeda member who is believed to have planned the attack on the USS *Cole*, Abdulrahim Mohammed Abda Al-Nasheri, was captured in 2002. Reportedly, he has provided information that supports concerns that terrorists plan to conduct additional maritime attacks. He confessed

Figure C-2: USS *Cole*
(*Source*: U.S. Navy Photo)

to planning attacks on shipping in the Strait of Gibraltar by using bomb-laden speedboat attacks against U.S. and British warships as they pass through the strait. Fortunately, the Moroccan intelligence service thwarted the plot.[257]

---

[254] Peter Chalk, "Threats to the Maritime Environment: Piracy and Terrorism," (RAND Stakeholder Consultation, Ispra, Italy 28-30 October 2002): 12.

[255] Bob Newman, "Terrorists Feared to Be Planning Sub-Surface Naval Attacks," *CNS News.com,* 3 December 2002; available from http://www.cnsnews.com/ForeignBureaus/archive/200212/FOR20021203a.html; Internet; accessed 19 March 2004.

[256] Ibid., 2.

[257] Michael Richardson, "A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction," *Viewpoints* (25 February 2004): 8; available from http://www.iseas.edu.sg/viewpoint/mricsumfeb04.pdf; Internet; accessed 5 April 2004.

Tactics and Techniques

Bombing

Bombs are the favored weapon for terrorists[258] for a variety of reasons. They are highly destructive, are flexible enough to be tailored to the mission, do not require the operator to be present, and have a significant psychological impact. To demonstrate their prominence in terrorist operations, 324 out of 482 total terrorist incidents or planned acts in the U.S. between 1980-2001 were bombings,[259] and 119 of 208 international terrorist incidents in 2003 were bombings.[260]

Bombs have a significant historical record, and a particular place in early anarchist and revolutionary thought, where dynamite was viewed as the equalizing force between the state and the individual.[261] There is little question that terrorist groups have a wealth of knowledge about building and planting these devices. As stated earlier in Chapter 3 of the handbook, the interaction between groups using both the Internet and through common training sites has facilitated the proliferation of effective devices and tactics throughout the terrorist network.

Bombings may be used as a technique to conduct other operations, such as sabotage or assassination, or can simply be a tactic to cause terror through the destruction and casualties produced by an explosion. Terrorists often use them to demonstrate how vulnerable the population truly is to attacks regardless of measures taken by a government to protect them.

Methods of delivering bombs are only limited by the imagination of the group planning the attack, and the capabilities of the individual bomb manufacturer. In recent history, directional bombs disguised as bricks in roadside walls and radio command detonated were used in the Israeli-occupied territories. The IRA has developed methods of remote detonation using police laser speed detection devices that can detonate a bomb programmed to respond to a particular laser pulse within line of sight, and that is immune to the usual electronic countermeasures for radio controlled bombs.[262]

Figure C-3 Car Bomb
(*Source*: U.S. Army Photo)

Car bombs commonly referred to as vehicle borne improvised explosive devices (VBIED), are also a very common method used by terrorists to deliver a bomb to its target. Besides the use of airplanes as VBIEDs on 11 September 2001 to hit the World Trade Center and the

---

[258] *Encyclopedia of World Terror*, 1997 ed., s.v. "Bombing."

[259] Department of Justice, Federal Bureau of Investigation, Counterterrorism Division, *Terrorism 2000/2001*, Report 0308, (Washington, D.C., 2004).

[260] Department of State, Office for Counterterrorism, *Patterns of Global Terrorism 2003* (Washington, D.C., April 2004, revised 22 June 2004), 5.

[261] Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 264-265.

[262] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 181.

Pentagon, probably the best-known domestic incident occurred on April 19, 1995, when a truck bomb exploded outside the Alfred P. Murrah building in Oklahoma City killing 168 people and injuring hundreds. Timothy McVeigh was convicted and later executed for the bombing. Overseas, the suicide truck bombing of the Marine Barracks in Beirut in October 1983 killing 241 Americans and the truck bomb that exploded near the Khobar Towers military barracks in Dhahran, Saudi Arabia on June 25, 1996 killing 19 people and injuring over 500 people are probably the most publicized incidents.

Although usually deployed as a single device, the Department of Homeland Security recently distributed a warning reflecting new tactics being used by terrorists in this area based on the bombings in Riyadh, Saudi Arabia in May 2003. These included terrorists hitting multiple targets, conducting simultaneous attacks, using multiple vehicles per target, and using assault/breaching personnel armed with small arms to accompany the VBIED to clear security personnel and gain access to the target area.[263]

In 2003, the use of bombs, and in particular improvised explosive devices (IEDs) reached an all time high in both lethality and employment techniques used by terrorists against their targets. Terrorists/insurgents have mastered the employment of roadside explosives to attack both individuals and motorcades/convoys. Many IEDs are bulky devices often made from artillery shells and detonated with garage door openers or doorbells. However, terrorists are now producing smaller devices that can be planted quickly and can be detonated from longer distances. Employment techniques include emplacing multiple devices along both sides of a road, sometimes disguised as trash or even hidden in animal carcasses that are daisy chained to explode simultaneously. Additionally, fake devices are often planted in an obvious spot to waste the time of explosive ordnance detachment personnel or to draw targets into an ambush.

Terrorist use of bombs is not restricted to roadside attacks or VBIEDs. Devices are often placed at a target site and then remotely detonated. One of the most recent terrorist bombing attacks occurred in Spain in March 2004. Ten backpack bombs with nails and screws packed around the explosives for shrapnel were detonated on four trains almost simultaneously using cell phones as the initiation device.[264] The results were nearly 200 dead and over 1,400 wounded. At the time of this writing, a multinational cell of al Qaeda loyalists is thought to be behind the bombings.

Appendix E contains descriptions of a variety of Improvised Explosive Devices (IEDs) that may be built by minimally competent terrorist groups. Appendix F discusses conventional weapons and unexploded ordnance (UXO) that can be adapted to use by terrorist organizations.

Arson

Arson is a destructive technique using fire, usually in sabotage operations against property. It permits a significant destructive effect with simple equipment and little training. It is one of

---

[263] National Security Institute, *Homeland Security Warns about Vehicle Bombs*, (Medway, MA, n.d.), 1-4; available from http://nsi.org/Library/Terrorism/Vehicle_Bombs.doc; Internet; accessed 14 January 2004.
[264] Lou Dolinar, "Cell Phones Jury-rigged to Detonate Bombs," *Newsday.com*, 15 March 2004; available from http://www.newsday.com/news/nationworld/ny-wocell153708827mar15,0,1644248.story?coll=ny-nationworld-headlines; Internet; accessed 15 March 2004.

the most commonly used methods of terrorist attack, ranking only behind bombing and assassination in total numbers covering the period 1980 - 1999.[265]

Since arson is primarily used against property, it is not normally considered as a casualty producer. However, arson can still result in fatalities, as an intentional or unintentional effect. Arson is most often used for symbolic attacks and economic effects. Single-issue groups, such as the Earth Liberation Front (ELF), particularly favor it for these purposes. Although ELF has claimed responsibility for dozens of arsons, probably the most costly arson committed by this group was in San Diego in August 2003.   Claiming it was targeting "rampant urban development," ELF started a fire that caused an estimated $50 million worth of damage in San Diego's fast-growing northern edge.[266]

Hoaxes, Misdirection and Compound Attacks

At the less lethal end of the spectrum, hoaxes can simply be methods to annoy and wear down security forces, and keep the population constantly agitated. Fake bomb threats, leaving suspicious items in public places, and talcum powder "anthrax" attacks bleed time and effort from other security operations, and contribute to uncertainty and fear.

Worse, such activities can be used to gain information about the target's response to a potential attack. Where the occupants go during the evacuation of a building, and how long it takes them to exit are useful elements of information in operational planning, and can be obtained through simply making an anonymous phone call or activating a fire alarm. Observation of regularly scheduled exercises or drills of emergency response procedures can provide similar information.

This technique can also be combined with an actual attack to circumvent fixed security measures. For example, the occupants of a bomb-resistant building with controlled access and a guard force could be forced to evacuate by a plausible, but false, threat. Many security plans would respect the potential danger such a threat represented, and evacuate the building. Unless properly secured, the evacuation has made the occupants more vulnerable to such weapons as a car bomb or other mass casualty techniques placed near the exits, or at a designated assembly point.

This tactic is taken one step further in a compound attack. If the unconfirmed threat of a bomb or arson will not generate the desired evacuation, an actual attack can be substituted. Using a standoff weapon such as a rocket launcher or mortar, the attack would be of short duration and need only be effective enough to force an evacuation to the more vulnerable area. If it can be obtained, knowledge of the targets' standard response to various types of attack permits the terrorist to craft a devastating two-step assault.

---

[265] Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999,* Report 0308, (Washington, D.C., n.d.), 41.

[266] Seth Hettena, "Earth Liberation Front Claims Responsibility for San Diego Arson," *The Mercury News*, 18 August 2003; available from http://www.mercurynews.com/mld/mercurynews/news/local/6562462.htm; Internet; accessed 17 March 2004.

A relatively recent example of a compound attack was the bombing in Bali on 12 October 2002, attributed to Jemaah Islamiyah, which is an Islamic terrorist group linked to al Qaeda. Initially, an electronically triggered bomb was detonated in a bar that forced the patrons out into the street. The compound attack was completed when a much more powerful car bomb was detonated in the street in front of another establishment. The result was 202 killed and 209 injured.[267]

Suicide Tactics

Suicide tactics are particular methods of delivering a bomb or conducting an assassination. They are defined as "An act of terror, employing an explosive or incendiary device that requires the death of the perpetrator for successful implementation."[268] It involves an individual wearing or carrying an explosive device into a crowded area or other target and then detonating it, or driving an explosive laden vehicle to a target and then detonating the device.

Suicide attacks are different in concept and execution from "high-risk" operations. In a high-risk mission, the *likely* outcome is the death of the terrorist(s), but mission success does not *require* that the participants die. The plan will allow for possible escape or survival of the participants, no matter how slim the chances. Using suicide as a tactic *requires* the death of the participant(s) in order to succeed.

A suicide bomber constitutes a highly effective precision-guided munition in the immediate tactical sense, but has a much greater impact from psychological considerations and the seemingly unstoppable nature of the weapon/tactic. There is no doubt that a suicide bombing can result in many casualties, cause extensive damage, attract wide media coverage, and usually guarantees that the attack will be carried out at the most appropriate time and place with regards to the circumstances at the target location.

Although a suicide bomber can be a lone terrorist working independently, the use of suicide terrorism as a tactic is normally the result of a conscious decision on the part of the leaders of terrorist organizations to engage this form of attack. It is frequently conducted as a campaign for a specific objective (e.g. withdrawal of foreign troops, interrupting peace negotiations).[269] It can often be a sign that a terror group has failed to meet it's goals through less extreme measures, and requires the tactical edge, as well as the potential inspiration to it's rank and file, that suicide bombing provides.[270] It can also indicate a specific operational requirement that can be met in no other way.

Although often associated with Middle Eastern religious groups, these type attacks are not unique to religious terrorist organizations or the Middle East. Both religiously motivated and secular groups have employed this tactic. Individual motivations on the part of the suicide

---

[267] *Wikipedia*, 2004 ed., s.v. "2002 Bali Terrorist Bombing;" available from http://en.wikipedia.org/w/wiki.phtml?title=2002_Bali_terrorist_bombing&printable=yes; Internet; accessed 17 March 2004.

[268] Martha Crenshaw, "Suicide Terrorism in Comparative Perspective," in *Countering Suicide Terrorism* (Herzilya, Israel: The International Policy Institute for Counter Terrorism, The Interdisciplinary Center, 2002), 21.

[269] Yoram Schweitzer, "Suicide Terrorism: Development and Main Characteristics," in *Countering Suicide Terrorism* (Herzilya, Israel: The International Policy Institute for Counter Terrorism, The Interdisciplinary Center, 2002), 85.

[270] Ehud Sprinzak, "Rational Fanatics," *Foreign Policy,* no. 120 (September/October 2000): 66-73.

assets themselves include religious or political convictions, hatred, and being coerced by the terrorist group into the attack. In addition to the Middle East; suicide attacks have been conducted in India, Panama, Algeria, Pakistan, Argentina, Croatia, Turkey, Tanzania, Kenya,[271] Chechnya, Russia, and the United States. However, the single most prolific suicidal terrorist group is the Tamil Tigers (LTTE) in Sri Lanka. They are inspired not due to religious reasons, but more by a cultish devotion to their leader, Velupillai Prabhakaran.[272]

As in any other terrorist operation, extensive pre-operational surveillance and reconnaissance, exhaustive planning, rehearsals, and sufficient resources will be devoted to an operation employing suicide as a tactic.[273] Secrecy is critical in success of a suicide mission in order to maintain the element of surprise. As stated earlier in this handbook, suicide bombers are rarely lunatics working alone, but are usually members of a terrorist group that have been recruited, indoctrinated, and trained. The groups write the texts for the videos usually produced and broadcast after the attack, and take pictures that are used for propaganda posters.

Although historically a male-dominated arena, women are becoming more involved in conducting these type operations. In fact women participated in 30 to 40% of the LTTE's nearly 200 suicide bombings in Sri Lanka.[274] Suicide attacks have also been conducted by Chechnyan and Palestinian women, as well as attacks conducted by women in Iraq, Turkey and Morocco. Additionally an FBI report has expressed concern over the forming of al Qaeda female units.[275]

Another trend is the use of teenagers in terrorist attacks. Palestinian teenagers have been involved in attacks against Israel for over three years. In February 2004, three boys, ages 13, 14, and 15 were arrested because they were planning to carry out an attack in the northern Israeli town of Afula. However, use of children and teenagers in suicide attacks became evident on March 16, 2004, when an 11-year-old boy was stopped at an Israeli checkpoint with a bomb in his bag. Although it is believed that the boy was unaware of the bomb, later that month a 14-year-old was stopped at a checkpoint wearing a suicide explosive vest.[276]

A typical operation involving suicide can require numerous personnel in support, some for extensive periods of time. A specialized suicide operation, such as assassination, might require 60 or more personnel, and sophisticated agent handling techniques. These support personnel are used to provide accommodations, transport, food, clothing and security for the

---

[271] "Suicide Terrorism: a Global Threat," *Jane's Intelligence Review* (October 2000): 1; available from http://www.janes.com/security/international_security/news/usscole/jir001020_1_n.shtml; Internet; accessed 20 January 2004.

[272] "Suicide Terrorism," *The Economist* (January 2004): 3; available from http://quicksitebuilder.cnet.com/supfacts/id396.html; Internet; accessed 17 March 2004.

[273] Rohan Gunaratna, "Suicide Terrorism: a Global Threat," *Jane's Intelligence Review* (20 October 2000): 1-7; available from http://www.janes.com/security/international_security/news/usscole/jir001020_1_n.shtml; Internet; accessed 7 September 2002.

[274] Clara Beyler, "Messengers of Death – Female Suicide Bombers," *International Policy Institute for Counter-Terrorism* (February 2003): 3; available from http://www.ict.org.il/articles/articledet.cfm?articleid=470; Internet; accessed 18 March 2004.

[275] Clara Beyler, "Female Suicide Bombers – An Update," *International Policy Institute for Counter-Terrorism* (March 2004): 1; available from http://www.ict.org.il/articles/articledet.cfm?articleid=508; Internet; accessed 31 March 2004.
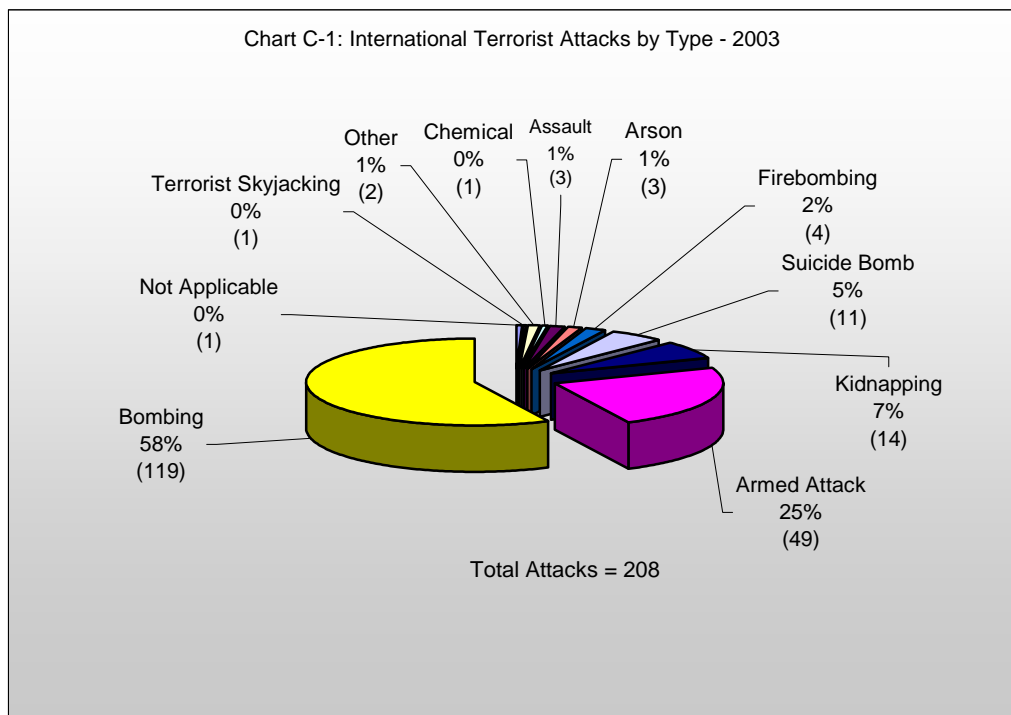
[276] Greg Myre, "Palestinian Bomber, 14, Thwarted before Attack," *International Herald Tribune* (March 2004): 1; available from http://www.iht.com/articles/511745.html; Internet; accessed 26 March 2004.

bomber until he/she reaches the target. Resident agents also help provide intelligence for the operation and cell members confirm the intelligence.[277]

The first major suicide bombing that struck at U.S. military forces was Hizballah's attack on the Marine barracks in Lebanon in October 1983 where 241 Americans were killed. Suicide attacks have also been used against coalition forces in Iraq during Operation Iraqi Freedom (OIF). On 27 December 2003, 12 Iraqis and six coalitions troops were killed, and 100 Iraqis and 26 coalition troops were wounded when four suicide bombers conducted coordinated attacks in the city of Kabala.[278] Unfortunately, these type attacks have continued in Iraq, with no sign of relief in the near future.

International Incidents – 2001-2002

Chart C-1 below, based on data from the State Department's 2003 *Patterns of Global Terrorism*, shows the various types of international terrorist attacks recorded during the

Chart C-1: International Terrorist Attacks by Type - 2003

Other 1% (2)
Chemical 0% (1)
Assault 1% (3)
Arson 1% (3)
Terrorist Skyjacking 0% (1)
Firebombing 2% (4)
Not Applicable 0% (1)
Suicide Bomb 5% (11)
Kidnapping 7% (14)
Bombing 58% (119)
Armed Attack 25% (49)
Total Attacks = 208

year.[279] Although the categories are somewhat different from this handbook, it does provide a real world representation of the various operations and tactics conducted by terrorists. As

---

[277] "Suicide Terrorism: a Global Threat," *Jane's Intelligence Review* (October 2000): 4-5; available from http://www.janes.com/security/international_security/news/usscole/jir001020_1_n.shtml; Internet; accessed 20 January 2004.

[278] Tom Lasseter, "Suicide Attackers Strike Karbala," *Knight Ridder,* 27 December 2003; available from http://www.realcities.com/mld/krwashington/news/special_packages/iraq/7581568.htm; Internet; accessed 20 January 2004.

[279] Department of State, Office for Counterterrorism, *Patterns of Global Terrorism 2003* (Washington, D.C., April 2004, revised 22 June 2004), 5.

stated above, bombs are the favorite weapon of terrorists, which is supported by the fact that 65% of the incidents involved some form of bombing.

Page Intentionally Blank

Appendix D
Firearms

…an international cabal of terrorists has the firepower to outgun the police of almost every western nation.

How Terrorists Kill: The Complete Terrorist Arsenal by J. David Truby

Terrorists use a variety of weapons to inflict their damage. As explained in the IRA General Headquarters pamphlet, they use explosives and almost any small arms weapon. These weapons can include submachine guns, grenades, pistols, automatic rifles, rifles, mortars, and rocket launchers.[280] Although some of these appear to be quite sophisticated for terrorists, they have become increasingly more available due to state sponsorship of many terrorist groups, regional conflicts, and a widespread illegal arms trade. In fact, many of the U.S. weapons captured from terrorists have been traced back to Vietnam.

When selecting weapons, terrorists look for 3 major factors: availability, simplicity, and efficiency. They like automatic weapons that can kill from a distance and have stopping power. They also want to be able to conceal the weapon, especially in urban terrain.[281]

As much as possible, terrorists do try to standardize calibers of their weapons for ease of ammunition resupply and they favor easily available military and semi-military weapons.[282] Most international terrorist groups like full automatic weapons, such as the AK47 and the M16. However, nearly any weapon can be found in use, especially in smaller groups. A favorite weapon by small groups in the United States is the 12-gauge shotgun.

Given the availability of weapons on the black market and the ever-changing technology, there is no way to develop a manual that would show every weapon a terrorist might use. This appendix is organized to review a representative example of various firearms used by terrorists today. It covers five basic types: pistols, submachine guns, assault rifles, sniper rifles, and shotguns.

Pistols are standard weapons for terrorists. They are small so they can be easily concealed. Most of them are lightweight and many modern pistols provide good firepower. Since their effective range is generally limited to about 50 meters, they do limit the distance to engage a target. However, they can be very effective at close range. They are more effective for personal security or victim control than for sustained firefights. Although the revolver is often considered more reliable, the semi-automatic provides more ammunition than a revolver

---

[280] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 111.

[281] Christopher Dobson and Ronald Payne, *The Terrorist: Their Weapons, Leaders, and Tactics* (New York: Facts on File, Inc, Revised Edition, 1982), 104.

[282] J. David Truby, *How Terrorists Kill: The Complete Terrorist Arsenal* (Boulder: Paladin Press, 1978), 7-8.

that only holds 6 bullets. Additionally, replacing a magazine is much faster than reloading a revolver's cylinder.

Submachine guns are basically short rifles that have a full automatic fire capability. They use pistol-caliber ammunition and typically have large magazine capacities. Their range, accuracy and penetration are better than pistols due to the longer barrel and sight radius. Submachine guns are a favorite with terrorist groups because they are small, light and easily concealed. They provide a large amount of firepower and are deadly at close range.

Assault rifles are the primary offensive weapons of modern militaries and are used extensively by terrorist organizations. In April of 2002, the Israeli Defense Forces seized a number of weapons in the West Bank. In that operation, 1,335 Kalashnikov rifles were recovered.[283] Assault rifles have calibers ranging from 5.45mm to 7.62mm and magazine capacities often in excess of 30 rounds. They normally have selective firing capability to allow single shot, 2 or 3 round bursts, or full automatic mode. Their effective ranges often exceed 600 meters and have effective rates of fire up to 400 rounds per minute in full automatic mode. When used by terrorists, the terrorist has the same firepower that a modern soldier has on the battlefield.

Since one of the major terror tactics is assassination, sniper weapons are often used to attack targets that are difficult to get close enough for other weapons. Additionally, with the development of large caliber sniper weapons, such as the Armalite AR-50 in .50 Caliber BMG, terrorists can also effectively engage light armored vehicles.

Although limited in range and penetration capability, shotguns are excellent weapons, especially for close-range assassinations or attacks. There is no requirement for precise aim since the dispersion effect of the large number of pellets will cover a wide area. They are readily available and relatively inexpensive compared to other weapons. Additionally, the barrels can be sawed off to permit easy concealment.

---

[283] "Weapons of Terror," *ADL* (8 April 2002): 1; available from http://www.adl.org/israel/weapons_list.asp; Internet; accessed 8 January 2003.

Handguns

CZ 75 (Czechoslovakia)

	Ammunition Types	Typical Combat Load
(*Source:* MCIA-1110-001-93, *Infantry Weapons Identification Guide,* September 1992, 94)	9mm Parabellum	Magazine Capacity: 16

SYSTEM

A double-action semi-automatic pistol modeled after the Browning P-35. It can be carried cocked and locked and is considered a very accurate handgun. Its design has been copied frequently to produce such guns as the TZ75, EAA Witness, TA90, Springfield Armory P9, ITM AT84, ITM AT88, and Baby Eagle.

Weight (kg): 0.98
Length (mm): 203
Operation: Recoil operated double action.
Fire Mode: Semi-automatic

SIGHTS

Iron sights.

VARIANTS

CZ 75B, 75BD, 75DAO, 75 Police: available in 9mm Luger, 9x21mm, .40 S&W

CZ 75 Compact, 75D Compact, 75 Semi Compact: Available in 9mm Luger.

AMMUNITION

Name: 9mm Parabellum
Caliber/length: 9 x 19 mm
Effective Range (m): 50
Muzzle Velocity (m/s): 381

Glock 17 (Austria)

	Ammunition Types	Typical Combat Load
(*Source*: Photograph Courtesy of GLOCK, Inc.)	9mm Parabellum	Magazine Capacity: 10, 17, 19, 31

SYSTEM

A semiautomatic handgun originally adopted by the Austrian Army and Police. It has a unique safe action striker-fired trigger mechanism that sets the striker in the half-cocked position after each round. When firing, the shooter pulls the trigger, which disengages the trigger safety, then cocks the striker to the full cock position prior to firing. The Glock has a polymer frame and steel slides.

Weight (kg): .905
Length (mm): 186
Operation: Recoil operated double action.
Fire Mode: Semiautomatic

SIGHTS

Iron sights. Adjustable on competition models.

VARIANTS

Glock 17L: Competition version
Glock 18: 3 round burst version
Glock 19: Compact version
Glock 34: Competition version
Numerous other models in a variety of calibers.

AMMUNITION

Name: 9 mm Parabellum
Caliber/length: 9 x 19mm
Effective Range (m): 50
Muzzle Velocity (m/s): 350

Makarov Pistol (USSR/Russia)

	Ammunition Types	Typical Combat Load
(*Source*: *U.S. Army Special Forces Foreign Weapons Handbook*, January 1967, I-13)	9mm Makarov	Magazine Capacity: 8

SYSTEM	VARIANTS
A blowback operated, double action semiautomatic handgun that is extremely sturdy, simple to operate and maintain, and very reliable. It was designed for Soviet army officers and Soviet police. It is a Walther PP style weapon and provides good defense at short and medium distances. There are some disadvantages with this weapon, specifically the 9mm Makarov is considered to be underpowered. Additionally, the magazine capacity of 8 is low compared to other handguns available.	PMM: 9x18mm Izh 71: 9x17mm short/.380 ACP Baikal IJ 70: 9mm Makarov/.380 ACP

Weight (kg): .66
Length (mm): 160
Operation: Double action
Fire Mode: Semiautomatic

AMMUNITION

Name: 9mm Makarov
Caliber/length: 9 x 18mm
Effective Range (m): 50
Muzzle Velocity (m/s): 315

SIGHTS

Iron sites.

Ruger GP100 (United States)

	Ammunition Types	Typical Combat Load
(UNCLASSIFIED) (UNCLASSIFIED) Figure 13. (U) Ruger GP100 .357 Magnum Revolver (*Source*: (S/NF/WN/NC) DST-2660H-481-89, *Terrorist Weapons Handbook – Worldwide* (U), 15 December 1989, 13. Unclassified Extract.)	.357 Magnum .38 Special	Cylinder Capacity: 6

SYSTEM	VARIANTS
The Ruger GP100 is a rugged double-action revolver, available in fixed and adjustable sight models. It was designed specifically for the law enforcement and security communities. It can be field stripped very quickly for easy maintenance. Although it is chambered for the .357 Magnum, it can also fire the .38 Special cartridge.	GP-141 KGP-141 GP-160 KGP-160 GP-161 KGP-161
Weight (kg): 1.28 Length (mm): 238 Operation: Double action Fire Mode: Single shot	
	AMMUNITION
SIGHTS Adjustable iron sights.	Name: .357 Magnum Caliber/length: .357 Cal/33 mm Effective Range (m): 60 Muzzle Velocity (m/s): 442

Submachine Guns

Heckler & Koch MP-5 (Germany)

	Ammunition Types	Typical Combat Load
Neg. 510058 (UNCLASSIFIED) Figure 21. (U) MP5A2 and MP5A3 9-mm Submachinegun (*Source*: (S/NF/WN/NC) DST-2660H-481-89, *Terrorist Weapons Handbook – Worldwide* (U), 15 December 1989, 19. Unclassified Extract.)	9 mm Parabellum	Magazine Capacity: 10, 15, 30

SYSTEM A submachine gun with a recoil operated roller-locked bolt that fires from a closed position. Very accurate and reliable under adverse conditions with only a minimum requirement for maintenance. The smooth recoil characteristics provide optimum control when firing bursts or when firing full automatic. It is very conducive for concealed carrying or for use in confined areas. Weight (kg): 3.07 loaded Length (mm): 490/660 Cyclic Rate of fire (rd/min): 800 Operation: Blowback Fire Mode: Semi-automatic, Full automatic SIGHTS Post front, select range peep rear. Night sights, scopes, laser aiming devices available.	VARIANTS MP5A1 – w/o stock MP5A2 – fixed polymer stock MP5A3 – telescopic metal stock SD1 – SD3 – same as above with internal silencers MP5N – US Navy model with 3 round burst capability AMMUNITION Name: 9 mm Parabellum Caliber/length: 9 x 19 mm Effective Range (m): 200 Muzzle Velocity (m/s): 400

PM 63 (Poland)

	Ammunition Types	Typical Combat Load
  (Source: USAREUR Pam 30-60-1, Identification Guide, Part One: Weapons and Equipment, East European Communist Armies, Volume 1: General, Ammunition and Infantry Weapons, September 1972, 70)	9 mm Makarov	Magazine Capacity: 15, 25

SYSTEM

The PM 63 is a blowback operated SMG that fires from the open bolt position. Although it is capable of both semi-automatic and full automatic modes, there is no selector switch. The semi-automatic mode is achieved by a short pull of the trigger, whereas full automatic requires pulling the trigger completely. It was designed with Special Forces in mind and was one of the lightest SMGs when it was introduced. It has been used by Polish Special Forces, police and by military personnel requiring a compact weapon. Iranian terrorists used it during the siege of the Iranian embassy in London in 1980. It has been a very prolific weapon, with tens of thousands being produced.

Weight (kg): 2.0 Loaded
Length (mm): 333/583
Cyclic Rate of fire (rd/min): 650
Operation: Blowback, firing from open bolt position
Fire Mode: Semi-automatic, Full automatic

SIGHTS

Iron sights that can be set on 75 or 150 meters.

VARIANTS

9mm Parabellum developed in 1971.

Unlicensed copy by NORINCO of China.

AMMUNITION

Name: 9mm Makarov
Caliber/length: 9 x 18 mm
Effective Range (m): 75
Muzzle Velocity (m/s): 320

Uzi (Israel)

	Ammunition Types	Typical Combat Load
(*Source*: (S/NF/WN/NC) DST-2660H-481-89, *Terrorist Weapons Handbook – Worldwide* (U), 15 December 1989, 20. Unclassified Extract.)	9mm Parabellum	Magazine Capacity: 20, 25, 32

SYSTEM

The Uzi is a recoil operated, select fire submachine gun that fires from the open bolt position. It has a folding stock and can be equipped with silencers. The Uzi submachine gun is manufactured by IMI and has been adopted by more than 90 countries for their police and military. Special operations and security units to include the US Secret Service and the Israeli Sayeret (Special Forces) use the compact variants. It is considered one of the most popular SMGs in the world, with more than 10 million manufactured around the world.

Weight (kg): 4.0 loaded
Length (mm): 470/650
Cyclic Rate of fire (rd/min): 600
Operation: Blowback, firing from open bolt position
Fire Mode: Semi-automatic, Full automatic

SIGHTS

Front – Post; Rear – Aperture "L" Flip.
Tactical flashlights and laser aiming modules are available.

VARIANTS

Mini Uzi
Micro Uzi

AMMUNITION

Name: 9 mm Parabellum
Caliber/length: 9 x 19mm
Effective Range (m): 200
Muzzle Velocity (m/s): 400

Assault Rifles

AK 47 (Russia)

	Ammunition Types	Typical Combat Load
  (*Source*: *OPFOR Worldwide Equipment Guide*, TRADOC ADCSINT-Threats, September 2001, 1-4.1)	7.62 x 39 mm	Magazine Capacity: 30

SYSTEM	VARIANTS

A gas operated, selective fire assault weapon adopted by the Soviet Army in 1949. It came with both a fixed wooden stock and a folding metal stock, the AKS, which was issued to paratroopers and armor units. All of the Kalashnikov assault rifles are very dependable and produce a high volume of fire. They are one of the most prevalent weapons used by terror groups today.	AKS: short stock
	AKM: updated version of the AK 47
	Clones:
	  Sako/Valmet: Finland
	  Galil: Israel
	  R-4/R-4C: South Africa

Weight (kg): 4.876 loaded Length (mm): 870 Cyclic Rate of fire (rd/min): 600 Operation: Gas operated Fire Mode: Semi-automatic, Full automatic	AMMUNITION Name: 7.62 Caliber/length: 7.62 x 39 mm Effective Range (m): 300 Muzzle Velocity (m/s): 710
SIGHTS Iron sites.	

AK 74 (Russia)

	Ammunition Types	Typical Combat Load
  (*Source*: *OPFOR Worldwide Equipment Guide,* TRADOC ADCSINT-Threats, September 2001, 1-3)	5.45 mm	Magazine Capacity: 30

SYSTEM	VARIANTS
A gas operated assault weapon used by the Soviet Army. It is basically an AKM rechambered to fire a 5.45mm round. It has a higher muzzle velocity than the AK 47/AKM, which gives it a longer effective range. It does not have the accuracy of the M16, but reportedly has better reliability in a combat situation and less maintenance requirements than the M16.	AKS 74: Folding stock version

SYSTEM

A gas operated assault weapon used by the Soviet Army. It is basically an AKM rechambered to fire a 5.45mm round. It has a higher muzzle velocity than the AK 47/AKM, which gives it a longer effective range. It does not have the accuracy of the M16, but reportedly has better reliability in a combat situation and less maintenance requirements than the M16.

VARIANTS

AKS 74: Folding stock version

Weight (kg): 3.6 loaded
Length (mm): 933
Cyclic Rate of fire (rd/min): 600
Operation: Gas operated
Fire Mode: Semi-automatic, Full automatic

AMMUNITION

Name: 5.45mm
Caliber/length: 5.45 x 39 mm
Effective Range (m): 500
Muzzle Velocity (m/s): 900

SIGHTS

Front: Post, Rear: U-notch

Night sights are available.

Colt M16 (United States)

	Ammunition Types	Typical Combat Load
(*Source*: US Army File Photo)	5.56mm (.223 Rem)	Magazine Capacity: 20, 30

SYSTEM	VARIANTS
A gas operated automatic assault rifle used by the US military as its primary weapon. Originally developed by Armalite as the AR 15, this was a scaled down version of the AR 10 redesigned to use the .223 Remington cartridge. It has been modified numerous times and is used by nearly 30 different militaries and is very popular with law enforcement agencies.	M16A1, A2, A3: Various upgrades. Civilian clones by Bushmaster, Armalite, Professional Ordnance, and many others.

SYSTEM

A gas operated automatic assault rifle used by the US military as its primary weapon. Originally developed by Armalite as the AR 15, this was a scaled down version of the AR 10 redesigned to use the .223 Remington cartridge.
It has been modified numerous times and is used by nearly 30 different militaries and is very popular with law enforcement agencies.

Weight (kg): 2.89 empty
Length (mm): 986
Cyclic Rate of fire (rd/min): 800
Operation: Gas operated
Fire Mode: Semi-automatic, Full automatic

SIGHTS

Iron sites. Scope capable.

VARIANTS

M16A1, A2, A3: Various upgrades.

Civilian clones by Bushmaster, Armalite, Professional Ordnance, and many others.

AMMUNITION

Name: 5.56 NATO
Caliber/length: 5.56 x 45mm
Effective Range (m): 460
Muzzle Velocity (m/s): 991

Sniper Rifles

ArmaLite AR 50 (United States)

	Ammunition Types	Typical Combat Load
(*Source*: Photo courtesy of ArmaLite*)	.50BMG	Single Shot

SYSTEM	VARIANTS
A single shot bolt action rifle that uses the.50 Cal Browning Machine Gun ammunition. It has a unique octagonal receiver bedded into a sectional aluminum stock and has a modified M-16 type pistol grip. The butt stock is fully adjustable and is removable for transport.	
Weight (kg): 19.24 with scope Length (mm): 1499 Operation: Bolt Action Fire Mode: Single shot	AMMUNITION Name: .50BMG Caliber/length: 12.7x99mm Effective Range (m): 1200 Muzzle Velocity (m/s): 865-890
SIGHTS ArmaLite sells this with a Leupold Mk4 10-power scope.	
* ArmaLite is a registered trademark of ArmaLite.	

Remington Model 700 (United States)

		Ammunition Types .223 Rem .308 Win	Typical Combat Load Magazine. Capacity: 5
(*Source*: US Army File Photo)			

SYSTEM	VARIANTS
A bolt action, magazine fed rifle that is basically a re-stocked Remington Model 700 VS varmint rifle. This is one of the most widely used tactical rifles in the United States. The police, the US Army and the US Marine Corps, use it.	M24 Sniper Weapon System (US Army) M40A1 Sniper Rifle (USMC)
Weight (kg): 4.08 empty without scope Length (mm): 1662 Operation: Bolt Action Fire Mode: Single Shot	AMMUNITION Name: .223 Rem/.308 Win Caliber/length: 5.56x45mm / 7.62x51mm Effective Range (m): 800 Muzzle Velocity (m/s): 1005 / 780-840
SIGHTS Variable telescopic scopes. No iron sights.	

Steyr-Mannlicher SSG-69 (Austria)

	Ammunition Types	Typical Combat Load
(UNCLASSIFIED) Neg. 529276 (UNCLASSIFIED) Figure 44. (U) Steyr SSG-69 7.62-mm Sniper Rifle (*Source*: (S/NF/WN/NC) DST-2660H-481-89, *Terrorist Weapons Handbook – Worldwide* (U), 15 December 1989, 32-33. Unclassified Extract.)	7.62 x 51mm (.308 Win)	Magazine. Capacity: 5

SYSTEM	VARIANTS
A bolt action, magazine fed rifle, which has been used as a sniper rifle by the Austrian forces, as well as many police agencies. The rifle is extremely accurate and has been used to win a number of international competitions.	
Weight (kg): 4.6 with scope. Length (mm): 1130 Operation: Bolt Action Fire Mode: Single shot	AMMUNITION Name: .308 Win Caliber/length: 7.62 x 51mm Effective Range (m): 800 Muzzle Velocity (m/s): 799 - 860
SIGHTS Scope	

Shotguns

Franchi SPAS 12 (Italy)

	Ammunition Types	Typical Combat Load
(UNCLASSIFIED) Figure 46. (U) Franchi SPAS 12-Gauge Shotgun (UNCLASSIFIED) (*Source*: (S/NF/WN/NC) DST-2660H-481-89, *Terrorist Weapons Handbook – Worldwide* (U), 15 December 1989, 34. Unclassified Extract.)	12 Ga. Shot 12 Ga. Buckshot 12 Ga. Slug	Tubular Magazine capacity: 8

SYSTEM

This is a dual mode shotgun, which can be operated both as a pump-action style shotgun and as a semi-auto shotgun. It can rapidly fire full power loads such as buckshot set on semi-auto, and can be switched to pump to handle low power rounds -- or if auto functioning fails to function properly. It has a relatively short barrel, which makes it suitable for operation in tight quarters. Both military and the police use it.

Weight (kg): 4.0
Length (mm): 1070
Operation: Pump or gas operated
Fire Mode: Semi-automatic

SIGHTS

Iron Blade

VARIANTS

AMMUNITION

Name: 12 Gauge
Caliber/length: 12 Ga/ 2 ¾ inch
Effective Range (m): 60
Muzzle Velocity (m/s): 393 (00 Buckshot)

Mossberg Model 500 (United States)

	Ammunition Types	Typical Combat Load
Figure 47. (U) Mossberg Model 500 12-Gauge Shotgun (*Source*: (S/NF/WN/NC) DST-2660H-481-89, *Terrorist Weapons Handbook – Worldwide* (U), 15 December 1989, 34. Unclassified Extract.)	12 Ga. Shot 12 Ga. Buckshot 12 Ga. Slug	Tubular Magazine capacity: 6, 8, 9

SYSTEM
This is a pump action shotgun that is common with the military and police departments, and is sold widely on the commercial market. It is available with both a traditional wood stock and with the pistol grip, as shown above.

Weight (kg): 2.6
Length (mm): 711
Operation: Pump Action
Fire Mode: Single shot

SIGHTS

Fixed iron sights

VARIANTS
Numerous variations of this model exist.

AMMUNITION

Name: 12 Gauge
Caliber/length: 12 Ga/ 2 ¾ inch and 3 inch
Effective Range (m): 60
Muzzle Velocity (m/s): 393 (00 Buckshot)

Page Intentionally Blank

Appendix E
Improvised Explosive Devices

Shampoo bottles, bicycle seats, tiffins [drinking/eating container]. A plastic container or an LPG cylinder. A parcel of books. A clock, a teddy bear. In the Kashmir Valley, any one of these innocuous objects can be fatal. They are all commonly used by militants to fashion bombs and improvised explosive devices (IEDs). But the most lethal of all is the remote controlled explosive device, hidden in a ditch, a drainpipe or a parked vehicle.

"Lethal Weapons", *Indian Express Newspaper* (Bombay), August 24, 2000

General

While terrorists will use conventional weapons, such as rocket-propelled grenades and assault rifles to achieve their goals, they also have the ability to assemble and employ a wide variety of lethal improvised explosive devices (IEDs). Explosives are a popular weapon with terrorists and are covered in the al Qaeda training manual. The manual states, "Explosives are believed to be the safest weapon for the Mujahideen. Using explosives allows them to get away from enemy personnel and to avoid being arrested." It goes on to say that, "In addition, explosives strike the enemy with sheer terror and fright." [284]

IEDs are a common tool of terror used by non-state actors. These devices have been fabricated in an improvised manner and incorporate highly destructive lethal and dangerous explosives or incendiary chemicals, which are designed to kill or destroy the target. The materials required for these devices are often stolen or misappropriated from military or commercial blasting supplies, or made from fertilizer and other readily available household ingredients.[285] IEDs basically include some type of explosive, fuse, detonators and wires, shrapnel and pieces of metal, and a container to pack the explosives and shrapnel.

The use of IEDs by terrorists is a constant threat. Terrorist groups are continuously developing new techniques and tactics in response to defenses and countermeasures established by their opponents. They will disguise IEDs to hinder recognition and will often booby-trap the devices to detonate if disturbed.

The most simple of the IEDs used is the one initiated by closing of a battery circuit, similar to turning on a battery operated light. When turning on the switch closes the circuit, electricity flows to the light so it can be illuminated. As shown in Figure E-1, a clothespin-triggering device in this IED replaces the light switch and when it is activated, the electricity flows to the charge, thus detonating the explosive.

---

[284] Ben N. Venzke and Aimee Ibrahim, *Al Qaeda Tactic/Target Brief* (Alexandria: IntelCenter/Tempest Publishing, 2002), 11.

[285] *Conventional Terrorist Weapons* (New York: United Nations Office for Drug Control and Crime Prevention, 2002)*,* 4*;* available from http://www.undcp.org/odccp/terrorism_weapons_conventional.html; Internet; accessed 12 November 2002.
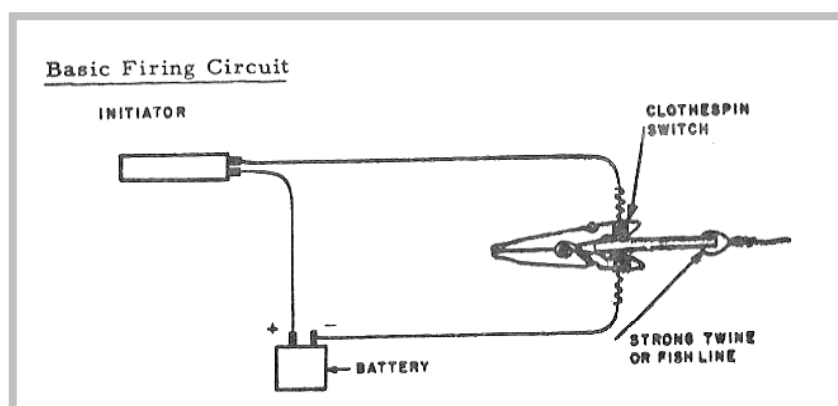
Figure E-1. Basic Firing Circuit (*Source*: TM 31-210)

The IED can be detonated using a number of triggering devices. These can be mechanical, electrical, or remote controlled type devices. For instance, after emplacing the IED, such as in a natural culvert or under a road by digging and then camouflaging the spot, the terrorist waits for the target to arrive. Once the target is within the damage area, the IED is initiated. The damage caused can be phenomenal as even a small amount of explosive can cause an explosion that dislodges a vehicle up to 50 feet in the air, or damage a bridge totally. This same scenario can be applied to a passenger train. More sophisticated assemblies of IEDs can be even more devastating and cause much damage.

Explosive Charges

Although terrorists use manufactured explosive material, it is easy for them to obtain the ingredients required to make improvised explosive material as well. The ingredients can be purchased at local stores with relative ease. Additionally, the instructions for making these type explosives have been published in a wide variety of literature, such as *The Anarchists Cookbook,*[286] for years. They are also available on the Internet. One such site has the recipes to make 27 different low and high order explosives[287] and another site gives instructions for both producing explosives and making the bombs.[288] The following are examples of common types of explosive charges found in IEDs.

- Improvised explosive mixtures: Although there are recipes to make virtually any explosive, the following are some common improvised ones that are used.

    - Ammonium nitrate fertilizer
    - Black powder
    - Gasoline
    - Match heads

---

[286] William Powell, *The Anarchist Cookbook* (Secaucus, NJ: Lyle Stuart, Inc., 1971), 111.

[287] *Improvised Explosives;* available from http://members.odinsrage.com/white88/18_ImprovisedExplosives.htm; Internet; accessed 11 December 2002.

[288] *Improvised Explosives*, vol. I*,* version 2.0 (15 May 1990); available from http://www.logicsouth.com/~lcoble/password/firearms.html; Internet; accessed 11 December 2002.

- Smokeless powder
- Sodium Chlorate and sugar

- Chemical reactions:
    - Acid bombs, such as nitric and sulfuric acid
    - Caustic bombs, such as Drano toilet bowl cleaner
    - Dry ice

- Plastic Explosives: This has become the explosive of choice for various international terrorist groups. There are 2 main types used by terrorists:
    - C-4: a white, RDX based explosive produced by the United States. This is the common plastic explosive used by the U.S. military.
    - SEMTEX: an orange, RDX and PETN based explosive produced in the Czech Republic. Intelligence experts estimated the bomb that destroyed Pan Am Flight 103 over Lockerbie, Scotland, in 1988 used about two-thirds pound of Semtex.[289]
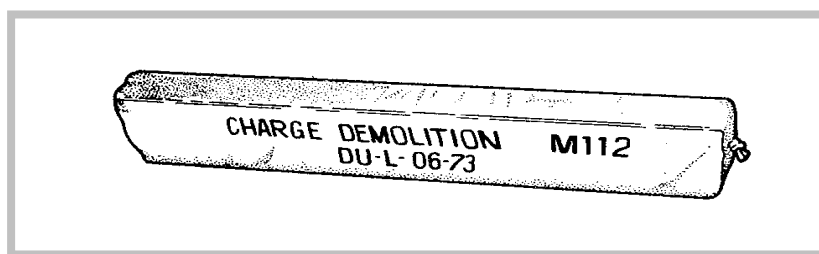
Figure E-2. U.S. Army M112 Block Demolition Charge of C4 (*Source*: FM 5-25)

- TNT: TNT is a most common military explosive, is used alone or as part of a composite explosive, and is a standard against which other military high explosives are rated.
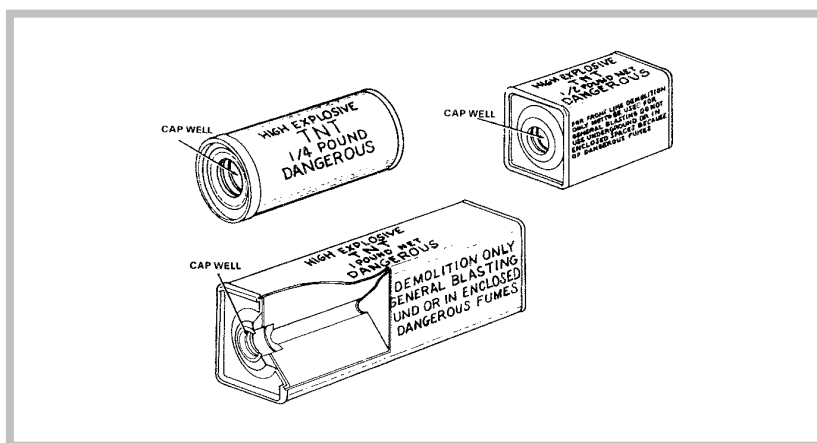
Figure E-3: TNT Block Demolition Charges (*Source*: FM 5-25)

- Dynamite: The most widely used explosive in the world for blasting operations. It has been fairly easy to obtain by both theft and legal purchases in the past.
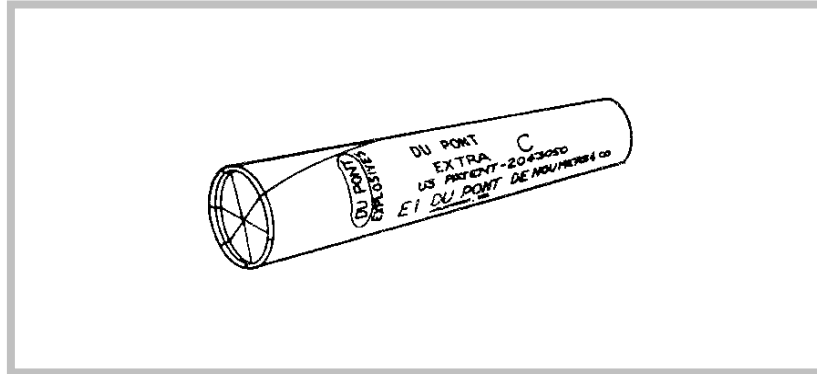
Figure E-4. Commercial Dynamite (*Source*: FM 5-25)

Common Trigger Devices

As mentioned earlier, some form of trigger is used to detonate the explosive device. These range from very simple homemade devices to highly technical devices. Although not all-inclusive, some examples are listed below.

- Manual wind-up alarm clocks and wristwatches. Delay can be up to 24 hours.
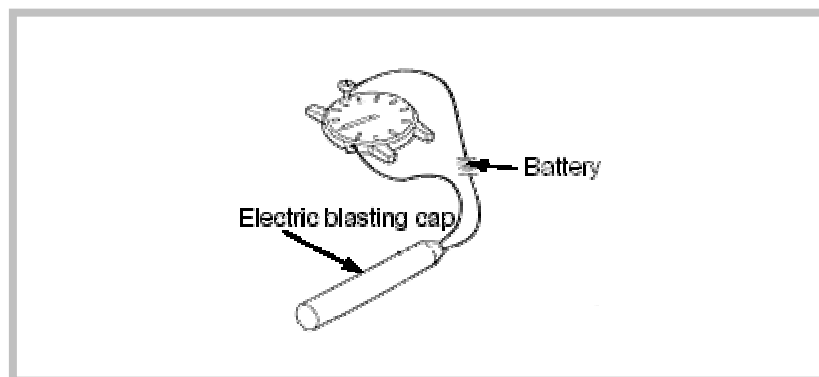
Figure E-5. Wristwatch Device (*Source*: FM 20-32)

---

[289] Earl Lane, "Plastic Explosives Difficult to Detect," *Newsday.com,* 23 July 1996, 1; available from http://www.newsday.com/news/nytwa96-jet3bomb,0,2501618.story; Internet; accessed 12 December 2002.

- Pressure release switch that is spring-loaded. These can be as simple as a mousetrap or a commercially produced switch.
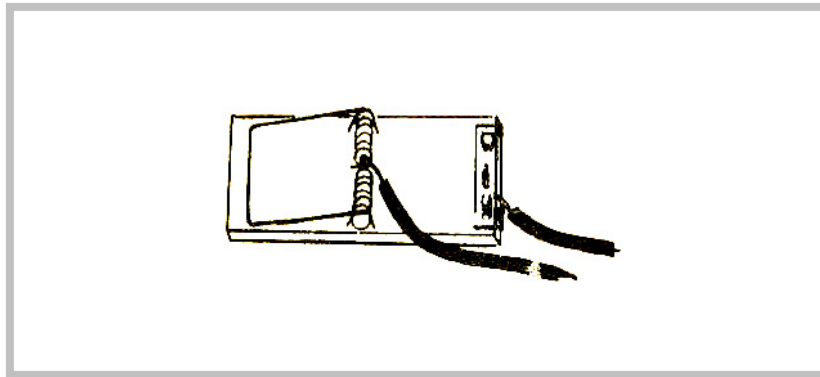
Figure E-6. Mousetrap Switch (*Source*: TM 31-210)

- Pull switches that actuate when a trip wire is pulled. There are many different forms of these triggers. They can be made easily by stripping the insulation off of wire and looping them together or by inserting a piece of wood between the contact wires on a clothespin.
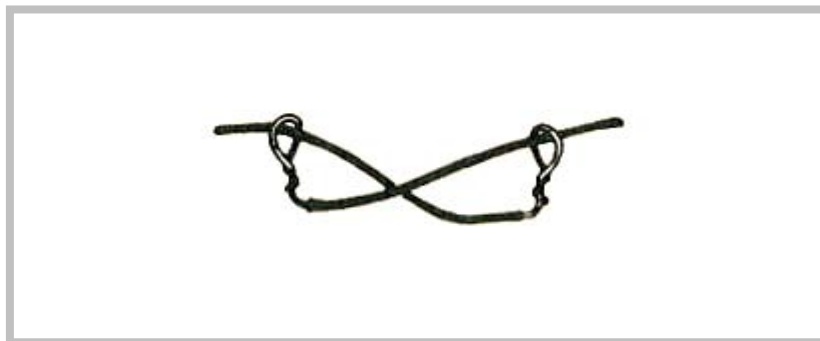
Figure E-7. Pull-Loop Switch (*Source*: TM 31-210)
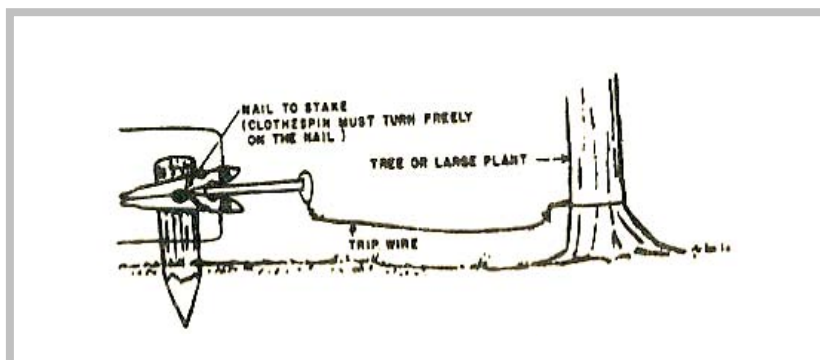
Figure E-8. Clothespin Switch (*Source*: TM 31-210)
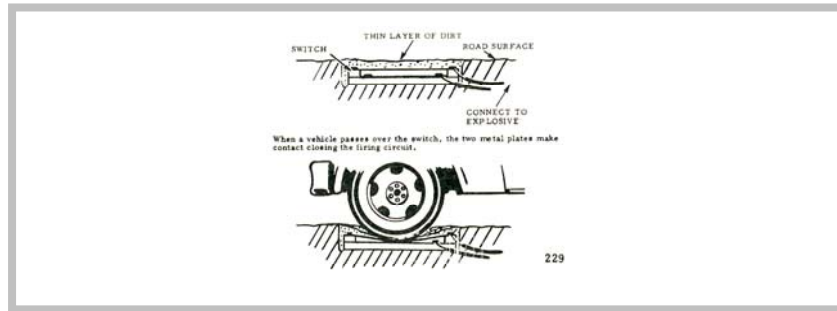
Figure E-9. Pressure Switch (*Source*: TM 31-210)
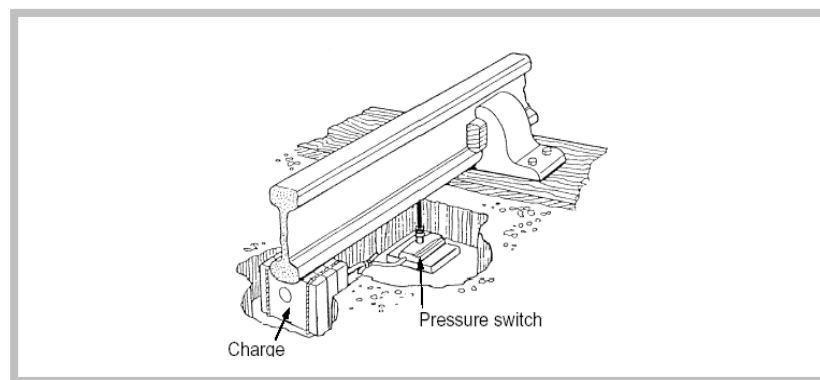
Figure E-10. Pressure Switch (*Source*: FM 20-32)

- Pressure switches that actuate when weight is applied.

- Metal Ball Switch: This switch will activate the device when it is tipped. It also can be used as an anti-disturbance type system that actuates the explosive device when it is disturbed.

Figure E-11. Metal Ball Switch (*Source:* TM 31-210)

- Barometric Sensor: Bombs can be triggered using a barometric sensor that detonates once it reaches a specific altitude. The bomb on Pan Am Flight 103 had a detonator with a barometric sensor with a timer delay and triggered only after the aircraft had reached a specific altitude and flew at that altitude for a set length of time.[290]
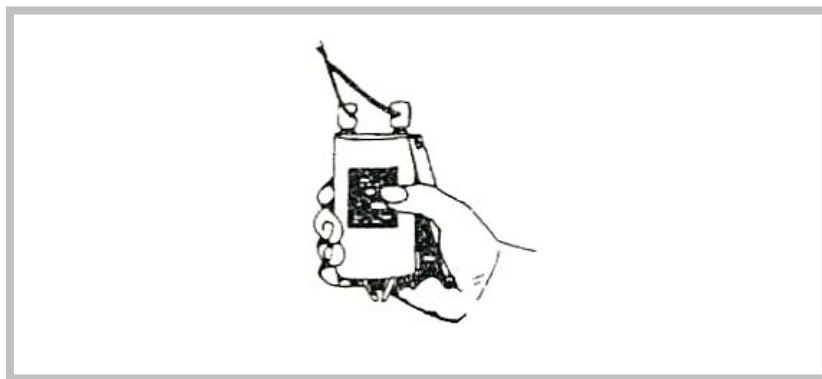
Figure E-12. Hand-held Detonation Device (*Source*: FM 20-32)

- Wire command detonation.

- Alarm equipment, such as motion detectors, infrared detectors, and heat detectors. Trigger devices were found in Chechnya that could discern the body heat of a person from background clutter over 20 feet away.[291]

- LED digital wristwatch.[292]

- Radio control systems similar to those used for models. These have been used by the IRA to detonate bombs against the British.[293]

- Hand-held radar guns. [294]

---

[290] Christopher Wain, "Lessons from Lockerbie," *BBC News,* 21 December 1998, 1; available from http://news.bbc.co.uk/1/hi/special_report/1998/12/98/lockerbie/235632.stm; Internet; accessed 12 December 2002.

[291] Ed Wagamon, "Tactical Combat in Chechnya: Mines & Booby Traps: The Number One Killer" (Part 1 of 2), *How They Fight: Armies of the World,* NGIC-1122-0062-01, vol 4-01 (August 2001): 35.

[292] Ibid., 35.

[293] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 180.

[294] Ibid., 181.

- Radio command detonation, such as battery-powered garage door openers, cell phones, and paging systems.[295]

Types of IEDs

The different types of IEDs vary based on the type explosive used, method of assembly, and also the method of detonation. As this is restricted only by human ingenuity, the types of IEDs are infinite. The Technical Support Working Group, which is an interagency group focusing on counter terrorism, categorizes IEDs based on their size and explosive capacity. The following table from *Jane's Unconventional Weapons Response Handbook* shows the categories.

Threat	*Explosives Capacity (TNT Equivalent)*
Firebomb or incendiary device	Less than 1 lb (0.5 kg)
Postal explosive device	1-5 lb (0.5 – 2.5 kg)
Pipe bomb	1-5 lb (0.5 – 2.5 kg)
Man-portable explosive device	5-50 lb (2.5 - 25 kg)
Compact sedan	500 lb (225 kg)
Full-size sedan	1,000 lb (455 kg)
Passenger or cargo van	4,000 lb (1,815 kg)
Small moving van or delivery truck	10,000 lb (4,535 kg)
Large moving van or water truck	30,000 lb (13,605 kg)
Semi-trailer	60,000 lb (27,210 kg)
Source: John P. Sullivan, et al., *Jane's Unconventional Weapons Response Handbook* (Alexandria, VA: Jane's Information Group, 2002), 53.	

Table E-1. Explosive Capacity

Although not all inclusive, some of the common IEDs a military organization will encounter are shown below:

- Pipe Bombs. This is a common type of terrorist bomb. Steel, iron, aluminum or copper pipes that are widely available in the market are used and low-velocity explosives are tightly capped inside. These are often wrapped with nails to cause more damage.

---

[295] Ed Wagamon, "Tactical Combat in Chechnya: Mines & Booby Traps: The Number One Killer" (Part 1 of 2), *How They Fight: Armies of the World,* NGIC-1122-0062-01, vol 4-01 (August 2001): 34.
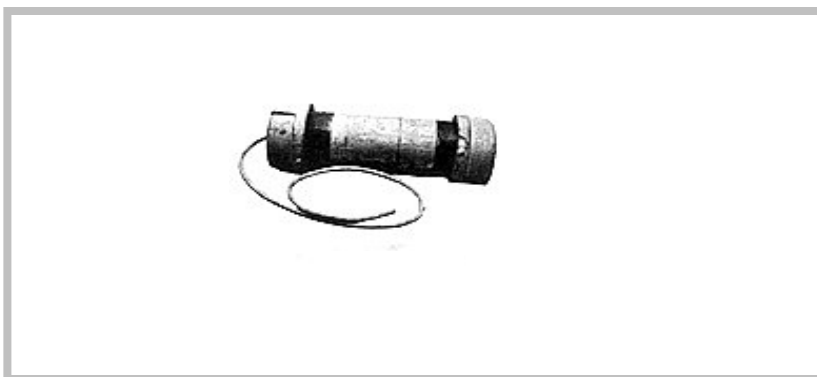
Figure E-13. Pipe Bomb (*Source:* BATF)

- Incendiary Devices. The Molotov cocktail was initially used by the Russian resistance against German armored vehicles in WWII. They are very easy to make, yet cause sever damage. The device normally consists of a glass bottle, which contains a very volatile fuel, such as gasoline or diesel. A cloth fuse is inserted through the bottle opening and is ignited before the bottle is thrown at the target.
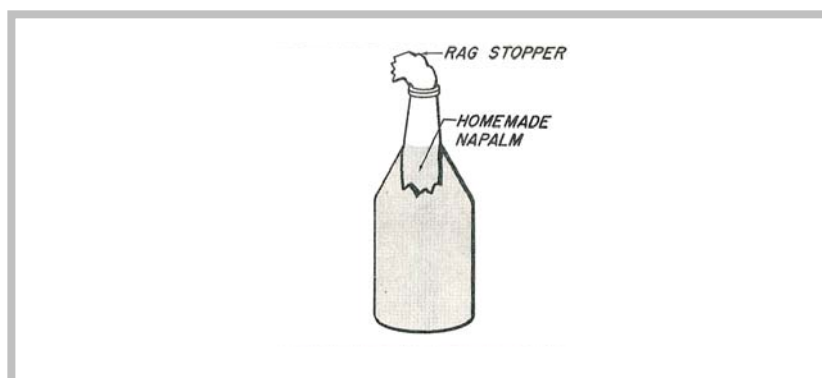

Figure E-14. Molotov Cocktail (*Source*: TM 31-201-1)

- Vehicle Devices. In addition to the IEDs, a vehicle can be modified to conceal and deliver large quantities of explosives to a target. The motive behind such incidents is to cause many casualties and gross property damage. This type of weapon is termed a VBIED (vehicle borne improvised explosive device). Factors encouraging VBIED use include:

  - Mobility.
  - Benign, non-threatening means of delivery and concealment.
  - Capacity to conceal large quantities of explosives.
  - Fragmentation and blast enhancement.
  - Penetration of target's perimeter not required (within reason).

- Minimal technology, logistics, and financing are needed to assemble a large explosive device proven to cause major personnel casualties and gross property damage.
- Suicide driver is nearly impossible to stop.

Such devices can also be remotely controlled for detonation. The near-simultaneous use of multiple VBIEDs against geographically dispersed targets has the potential to create mass casualties and panic.

- Other devices: The design of IEDs is only limited to the ingenuity of the person making them. A few examples of other type devices are shown in the accompanying illustrations.

Figure E-15. Dynamite/Nail Bomb (*Source*: BATF)
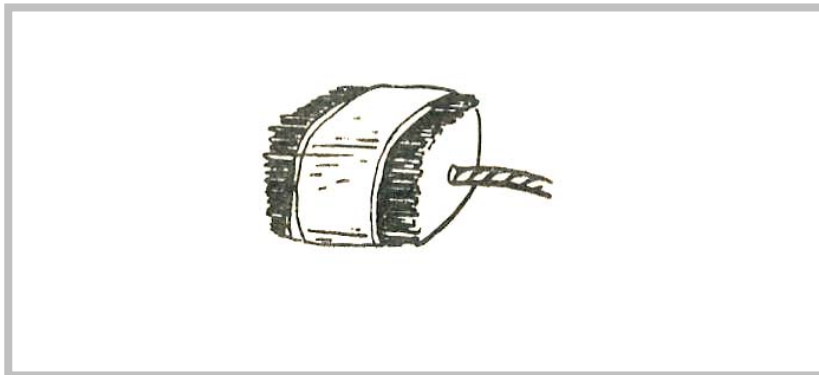
Figure E-16. Nail Grenade (*Source*: TM 31-210)

- Projected IEDs. These are improvised devices that launch some form of projectile at the intended target. These fall into 3 categories: Explosively formed projectiles (commonly called platter charges or disk charges); shoulder fired rocket launchers; and improvised mortars.

  - Platter charges. These are designed with some form of explosive material placed on one side of a flat metal plate. When the device is detonated, the metal plate is launched at the target and can penetrate armor and concrete.

- Shoulder fired rockets. These are very similar to military rocket launchers, such as the RPG. However, they are less accurate and have a shorter range.

Red Army Brigade Ambush
Alfred Herrhausen, 30 November 1989

The Red Army Brigade, primarily a German domestic terrorist group, targeted politicians and influential businessmen for murder. As head of Deutsche Bank, Germany's largest bank, Alfred Herrhausen was the most influential businessman in the country. The Red Army Brigade vowed to kill Herrhausen by the end of November 1989

Herrhausen was chauffeured to work each morning in an armored Mercedes, with bodyguards in a lead and a follow car. The Red Army Brigade learned his routine, which was to take substantially the same route to and from work at approximately the same time each day. That route went through a park, which made for an excellent surveillance and attack site. RAB members, in workers' clothes, dug a small hole across the road, set up an infrared beam on one side and a reflector on the other.

On 30 November 1989, Alfred Herrhausen headed for work in his usual motorcade, along his usual route, at his usual time. A RAB lookout signaled the triggerman that Herrhausen's motorcade was approaching the kill zone. The triggerman allowed the first car through, then activated the infrared beam. When Herrhausen's car broke the beam, a timer delay caused a plate charge hidden on the back of a bicycle to detonate, sending it through the rear door of Herrhausen's armored car. It severed his legs and he bled to death.

The plate charge was driven by 10 kilos (22 pounds) of TNT. It was a 5-pound, 8-inch copper plate. The TNT detonated at 18,000 feet per second, sending the plate into Herrhausen's body at 14,000 feet per second and demolishing the Mercedes.

Source: Diplomatic Security Surveillance Detection Program Course of Instruction, U.S. State Department, October 1999.

- Improvised mortars. A mortar system can be built using propane cylinders as the launch tube. Add a simple elevation system and detonator and a complete improvised mortar system can be obtained.

Figure E-17. Improvised Mortar System (*Source*: File Photo)
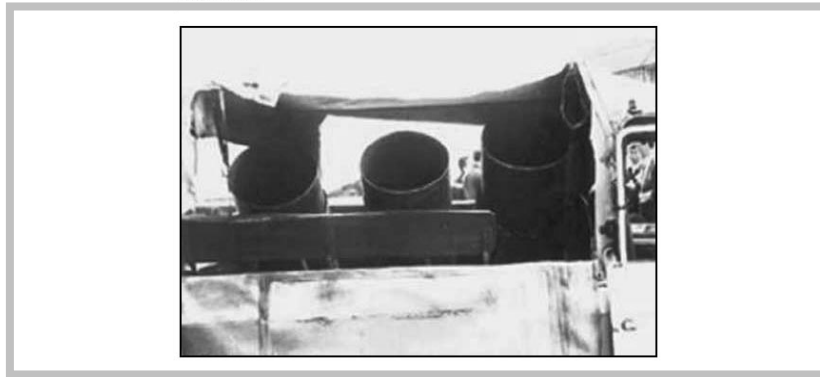
Figure E-18. Multi-tube Battery Mounted in Truck (*Source*: File Photo)

Commercial Product Modification

Terrorists also show great skill and creativity in their ability to weaponize commercial off the shelf products. Given the right components, something as benign as a cell phone can be turned into a weapon that becomes easy to conceal and to employ. In Figure E-19, the cell phone has been converted to a four-barreled gun.

Covert Firearms

Covert firearms can be developed or secretly obtained through black market channels. With the right amount of cash and good connections a terrorist can find or produce many dangerous and unexpected weapons for their arsenals of terror.

Figure E-19. Four-barreled
Cell Phone Gun
(Source: File Photo)
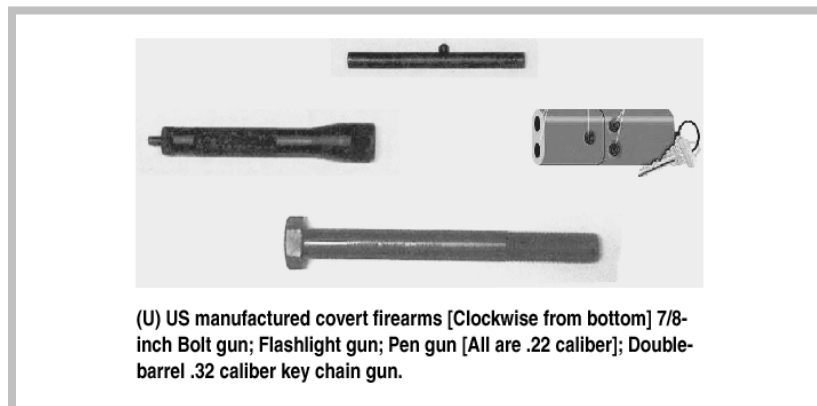
(U) US manufactured covert firearms [Clockwise from bottom] 7/8-inch Bolt gun; Flashlight gun; Pen gun [All are .22 caliber]; Double-barrel .32 caliber key chain gun.

Figure E-20. US Manufactured Covert Firearms (*Source*: File Photo)

Evacuation Distance Tables

There is no question that U.S. forces are susceptible to the threat posed by IEDs. When confronted with these type devices, trained personnel should only disable them. Friendly personnel should be evacuated to a safe distance to preclude casualties in case the IED is detonated. There are numerous references available covering the IED threat. Figure E-21 is an example of IED smart cards developed by CJTF-7 during OIF and Figure E-22 is an example of a reference guide developed by the Marine Corps. The Army also has GTA 90-01-001, Improvised Explosive Device (IED) and Vehicular Borne Improvised Explosive Device (VBIED) Smart Card, but this has restricted distribution. Table E-2 is representative of a card distributed by the Department of Defense that provides recommended evacuation distances based on the type IED.
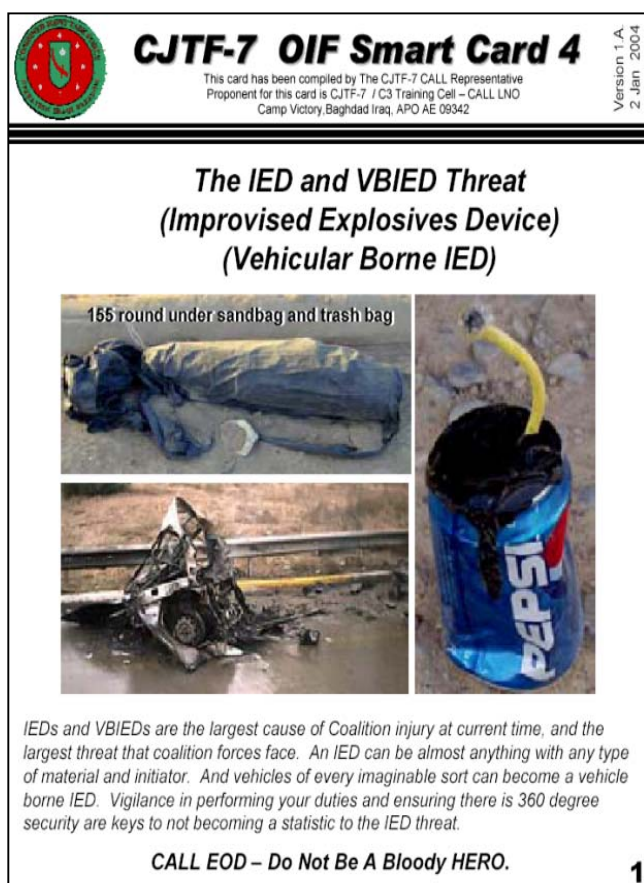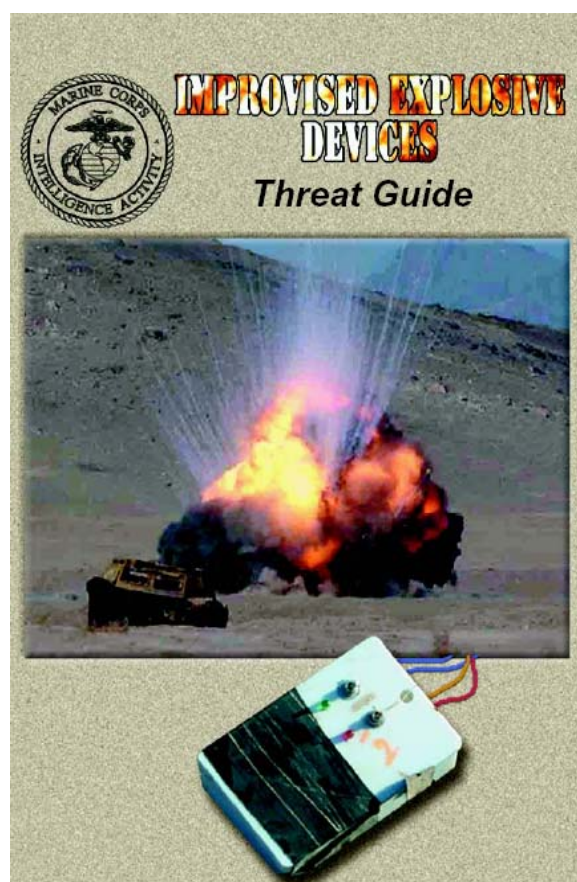

Figure E-21. CJTF-7 OIF Smart Card 4

Figure E-22. Marine Corps Intelligence Agency IED Threat Guide

THREAT	THREAT DESCRIPTION	EXPLOSIVES CAPACITY[1] (TNT EQUIVALENT)	BUILDING EVACUATION DISTANCE[2]	OUTDOOR EVACUATION DISTANCE[3]
	PIPE BOMB	5 LBS/ 2.3 KG	70 FT/ 21 M	850 FT/ 259 M
	BRIEFCASE/ SUITCASE BOMB	50 LBS/ 23 KG	150 FT/ 46 M	1,850 FT/ 564 M
	COMPACT SEDAN	500 LBS/ 227 KG	320 FT/ 98 M	1,500 FT/ 457 M
	SEDAN	1,000 LBS/ 454 KG	400 FT/ 122 M	1,750 FT/ 534 M
	PASSENGER/ CARGO VAN	4,000 LBS/ 1,814 KG	640 FT/ 195 M	2,750 FT/ 838 M
	SMALL MOVING VAN/DELIVERY TRUCK	10,000 LBS/ 4,536 KG	860 FT/ 263 M	3,750 FT/ 1,143 M

This card supersedes any previous undated versions 11/99
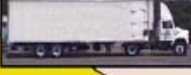
Terrorist Bomb Threat Stand-Off

THREAT	THREAT DESCRIPTION	EXPLOSIVES CAPACITY[1] (TNT EQUIVALENT)	BUILDING EVACUATION DISTANCE[2]	OUTDOOR EVACUATION DISTANCE[3]
	MOVING VAN/ WATER TRUCK	30,000 LBS/ 13,608 KG	1,240 FT/ 375M	6,500 FT/ 1,982 M
	SEMI-TRAILER	60,000 LBS/ 27,216 KG	1,570 FT/ 475 M	7,000 FT/ 2,134 M

All personnel must evacuate (both inside of buildings and out).

Building Evacuation Distance

Outdoor Evacuation Distance

Threat

All personnel must either seek shelter inside a building (with some risk) away from windows and exterior walls, or move beyond the Outdoor Evacuation Distance.

Preferred area (beyond this line) for evacuation of people in buildings and mandatory for people outdoors.

[1] Based on maximum volume or weight of explosive (TNT equivalent) that could reasonably fit in a suitcase or vehicle.
[2] Governed by the ability of an unstrengthened building to withstand severe damage or collapse.
[3] Governed by the greater of fragment throw distance or glass breakage/ falling glass hazard distance. Note that pipe and briefcase bombs assume cased charges which throw fragments farther than vehicle bombs.

Table E-2. Explosive Device Evacuation Distances (*Source*: DOD)

Appendix F
Conventional Military Munitions

The regional operational headquarters further disclosed that over the past 24 hours, 19 items of small arms, 9 grenade launchers, 3 machine guns and a large amount of ammunition, including 10 artillery shells and 18 landmines, have been found and seized in Chechnya. Also, over 83 kg of TNT has been found.

"ARMS CACHE FOUND IN GROZNY CEMETERY," *On-Line Pravda*, 10 August 2002

General

Although terrorists are known for using fabricated improvised explosive devices, they also use a wide variety of military conventional weapons. These weapons range all the way from highly sophisticated Stinger Missiles to booby-trapped unexploded ordnance. This appendix will review many of the weapons the military may encounter when dealing with the terrorist threat.

Fragmentation Grenades

Grenades are a common weapon used by terrorists. In fact, in the annual report published by HAMAS on terrorist activities in 1998, they stated that a combination of time delayed bombs coupled with commando attacks using hand grenades were the major part of effective operations and caused the most casualties.[296] Although terrorists will use any grenade they can acquire, some of the common grenades available are listed below. These figures are courtesy of the Naval Explosive Ordnance Disposal Technology Division.[297]

- Figure F-1. U.S. Grenade, Fragmentation, M2A1, M2A2, U.S. Army

Characteristics	
Color:	Olive drab
Length:	114mm
Width:	57mm
Weight:	453.6g
Filler:	TNT

---
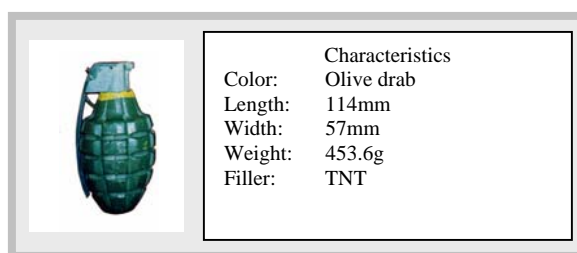
[296] Reuven Paz, *Hamas Publishes Annual Report on Terrorist Activity for 1998* (Herzliya, Israel: International Policy Institute for Counterterrorism, May 3, 1999), 1; available from http://www.ict.org.il/spotlight/det.cfm?id=259; Internet; accessed 6 December 2002.

[297] Department of Defense, Naval Explosive Ordnance Disposal Technology Division, *ORDATA II - Enhanced Deminers' Guide to UXO Identification, Recovery, and Disposal,* Version 1.0, [CD-ROM], (Indian Head, MD: Naval Explosive Ordnance Disposal Technology Division, 1999).

- Figure F-2. U.S. Grenade, Fragmentation, M26, M26A1, M61

Characteristics
Color: Olive drab with yellow markings
Length: 99mm
Width: 57mm
Weight: 453.6g
Filler: Composition B

- Figure F-3. French Grenade, Fragmentation, TN 733

Characteristics
Color: Olive drab with yellow markings
Length: 94mm
Width: 52mm
Weight: 265g
Filler: Composition B

- Figure F-4. U.K. Grenade, Fragmentation, No. 36M MK1

Characteristics
Color: Black or varnished brown
Length: 102mm
Width: 61mm
Weight: 773g
Filler: Amatol

- Figure F-5. Spanish Grenade, Fragmentation, POM 1

| Characteristics |
|---|
| Color: Black and unmarked |
| Length: 131mm |
| Width: 55mm |
| Weight: 335g |
| Filler: TNT |

- Figure F-6. U.S.S.R. Grenade, Hand, Defensive, RGD-5
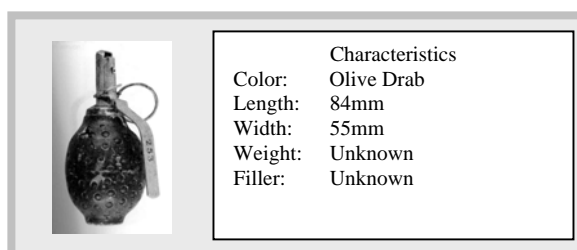
Characteristics
Color: Olive drab with black markings
Length: 117mm
Width: 58mm
Weight: 320g
Filler: TNT

- Figure F-7. U.S.S.R. Grenade, Hand, Defensive, F1

Characteristics
Color: Gray, olive drab or unpainted
Length: 117mm
Width: 55mm
Weight: 699g
Filler: TNT
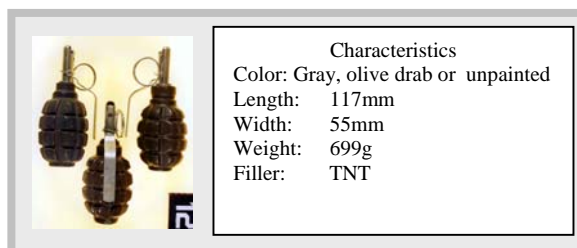
- Figure F-8. North Korean Grenade, Fragmentation, Model Unknown

Characteristics
Color: Olive Drab
Length: 84mm
Width: 55mm
Weight: Unknown
Filler: Unknown

- Figure F-9. Chinese (P.R.) Grenade, Fragmentation, Type 86P

Characteristics
Color: Olive green
Length: 90mm
Width: 52mm
Weight: 260g
Filler: PETN
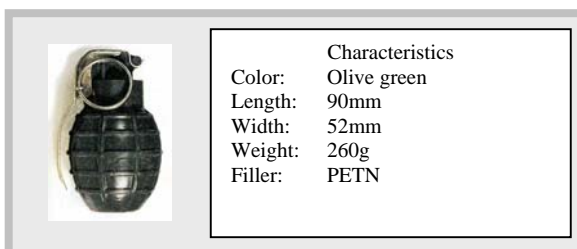
Rocket Propelled Grenade

This weapon fires a motorized grenade from a tube-like launcher. Although it is an unguided weapon, a trained operator can negotiate targets at a long distance. Even though it was originally developed for an anti-tank weapon system, many terrorists use them as anti-aircraft weapons. RPGs were used to bring down two MH-47 Chinook helicopters in the Shah-e-Kot area of Afghanistan in 2002 and the same system was used in 1993 in Mogadishu, Somalia, when Somalis firing RPGs brought down a pair of UH-60 Black Hawk helicopters. Many armies use these systems and they are widely available on the weapons black market.

- Russian 40mm Anti-tank Grenade Launcher RPG-7V. The RPG-7V is abundant throughout the terrorist world and is being used extensively by terrorist organizations in the Middle East and Latin America and is thought to be in the inventory of many insurgent groups. The RPG-7V is a relatively simple and functional weapon, with an effective range of approximately 500 meters when used against a fixed target, and about

300 meters when fired at a moving target. [298] It can penetrate 330mm of armor. Photo is from the TRADOC *Worldwide Equipment Guide* (WEG).
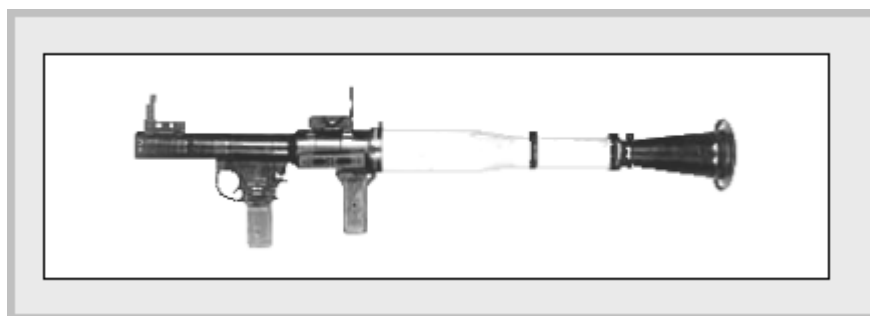

Figure F-10. RPG-7V Antitank Grenade Launcher (*Source:* WEG)

- U.S. 66mm Light Anti-tank Weapon M72 LAW. Although the M72-series LAW was mainly used as an anti-armor weapon, it may be used with limited success against other targets such as buildings and light vehicles. It's effective range is not as good as the RPG-7V, since it's only effective to 200 meters for stationary targets, and 165 meters for moving targets. It can penetrate 350mm of armor.
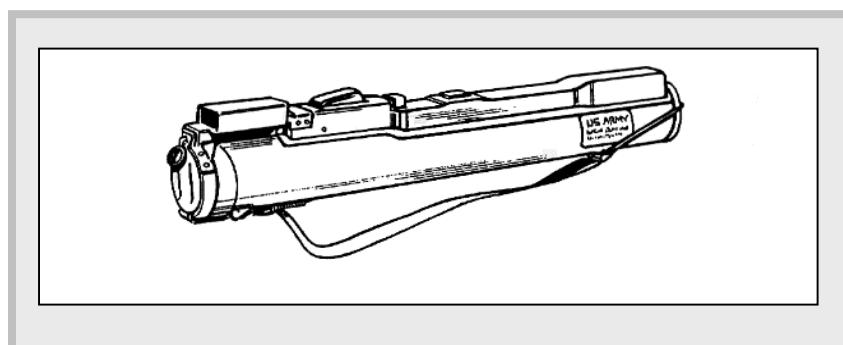
Figure F-11. M72 Series Light Antitank Weapon (*Source:* FM 23-25)

Air Defense Weapons

Although there are a myriad of air defense weapon systems, the man portable systems are the ones that will be covered in this section. As the name indicates, these systems are portable and can be employed by terrorists very quickly. Due to excellent performance and the large number of these air defense systems throughout the world, the two systems discussed below represent some of the most formidable threats to aircraft of all types. The fact that terrorists will use these weapons was demonstrated in November 2002 when two surface-to-air missiles

---

[298] *Conventional Terrorist Weapons* (New York: United Nations Office for Drug Control and Crime Prevention, 2002), 3; available from http://www.undcp.org/odccp/terrorism_weapons_conventional.html; Internet; accessed 12 November 2002.

were fired at a Tel Aviv bound Arkia airlines Boeing 757 as it departed Mombasa, Kenya. Fortunately the missiles missed their target, but it is an indication of possible employment of the systems in the future.

- U.S. FIM92A Stinger. The US-made Stinger is a man-portable infrared-guided shoulder-launched Surface-To-Air Missile (SAM). It proved to be highly effective in the hands of Afghan Mujahedeen guerrillas during their insurgency against the Soviets. Its maximum effective range is approximately 4,000+ meters. Its maximum effective altitude is approximately 3,500 meters. It has been used to target high-speed jets, helicopters, and commercial airliners.
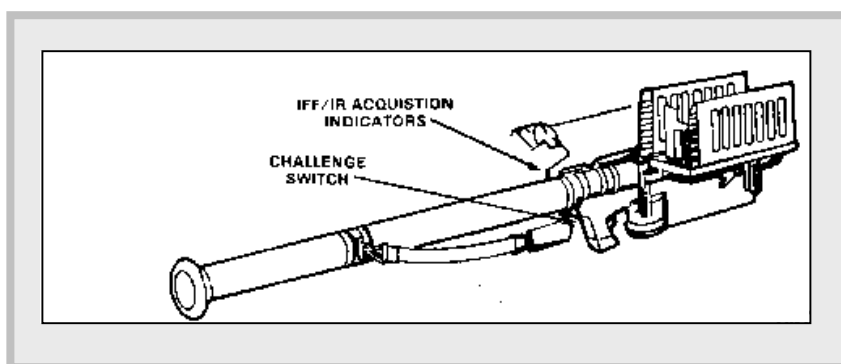
Figure F-12. U.S. FIM92A Stinger (*Source*: FM 44-18-1)

- Russian SA 7b/Grail. Sold by the thousands after the demise of the former Soviet Union, the SA-7 "Grail" uses an optical sight and tracking device with an infrared seeking mechanism to strike flying targets. Its maximum effective range is approximately 5,500 meters and maximum effective altitude is approximately 4,500 meters. It is known to be in the stockpiles of several terrorist and guerrilla groups.
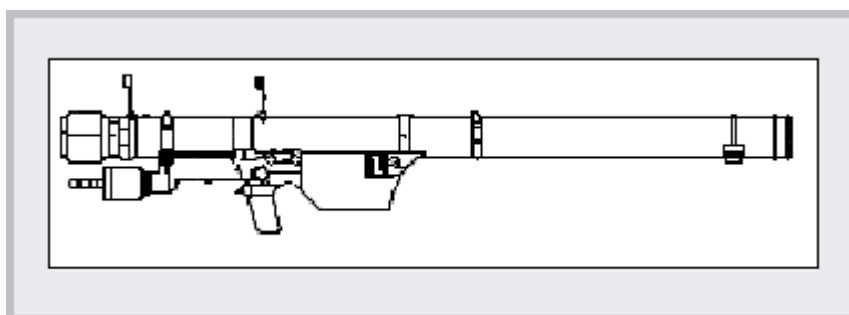
Figure F-13. Russian SA 7b/Grail (*Source:* WEG)

Bombs and Artillery

Although most bombs used by terrorists are fabricated devices, they do use some conventional munitions, especially as booby traps. They often use unexploded ordnance and modify it for their purposes. A 2001 report from the United Nations Mine Action Coordination Center on the former Yugoslav Republic of Macedonia indicates a plethora of unexploded munitions, to include 122 mm artillery rounds, 100 mm tank rounds, 82 mm and 120 mm mortar rounds, 20 mm and 30 mm cannon rounds, and 50 mm rocket rounds.[299] The following reflects some common munitions used by terrorist organizations. These figures are courtesy of the Naval Explosive Ordnance Disposal Technology Division.[300]

- Figure F-14. U.S. Artillery Projectile, 105mm, HE, M1

Characteristics
Color: Olive drab with yellow markings
Length: 404mm
Width: 105mm
Weight: 18.11kg
Filler: Composition B

- Figure F-15. U.S. Artillery Projectile, 155mm, HE, M107

Characteristics
Color: Olive drab with yellow markings
Length: 605mm
Width: 155mm
Weight: 42.91kg
Filler: Composition B

---

[299]C.J. Clark, *Mine/UXO Assessment: Former Yugoslav Republic of Macedonia* (New York: United Nations Mine Action Coordination Center, 8 October 2001), 2; available from http://www.mineaction.org/sp/mine_awareness/_refdocs.cfm?doc_ID=707; Internet; accessed 13 December 2002.

[300] Department of Defense, Naval Explosive Ordnance Disposal Technology Division, *ORDATA II - Enhanced Deminers' Guide to UXO Identification, Recovery, and Disposal,* Version 1.0, [CD-ROM], (Indian Head, MD: Naval Explosive Ordnance Disposal Technology Division, 1999).

- Figure F-16. U.S.S.R. Artillery Projectile,
  122mm, HE, FRAG,
  Model OF-472

Characteristics
Color: Dark gray with black markings
Length: 564mm
Width: 122mm
Weight: Not available
Filler: TNT

- Figure F-17. U.S.S.R. Projectile,
  100 mm, HEAT-FS,
  Model ZBK-5M

Characteristics
Color: Steel with copper rotating bands
Length: 649 mm
Width: 100 mm
Weight: 12.40 kg
Filler: RDX
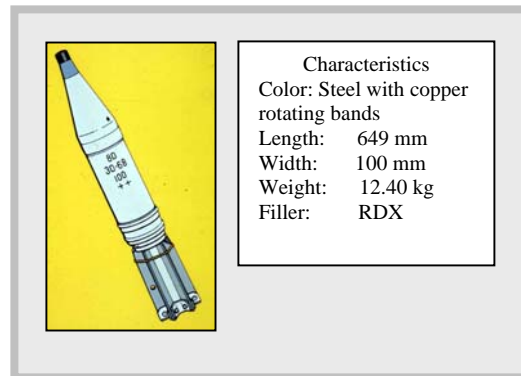
- Figure F-18. U.S.S.R. Projectile,
  120 mm, Mortar, HE-FRAG,
  Model OF-843A

Characteristics
Color: Silver painted body with black markings
Length: 615 mm
Width: 120 mm
Weight: Unknown
Filler: Amatol
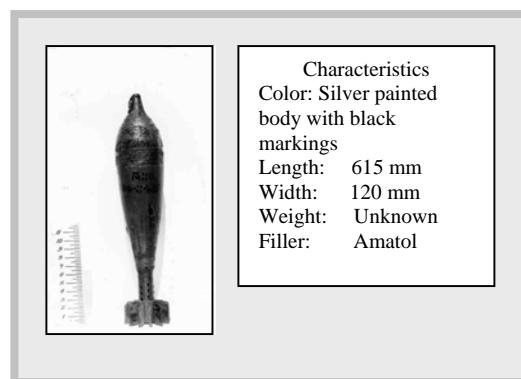
- Figure F-19. U.S. Bomb, 220 lb, Fragmentary, AN-M88

Characteristics
Color: Olive drab with yellow band
Length: 1.1m
Width: 206mm
Weight: 99.79kg
Filler: Composition B

- Figure F-20. U.S. Bomb, 250 lb, GP, AN-M57 & AN-M57A1

Characteristics
Color: Olive drab with yellow band
Length: 1.15m
Width: 276.86mm
Weight: 117.94kg
Filler: Amatol

- Figure F-21. U.S. Bomb, 500 lb, GP, MK3, MOD 1

Characteristics
Color: Gray overall with yellow disc
between lugs
Length: 1.51m
Width: 355.6mm
Weight: 228.61kg
Filler: TNT
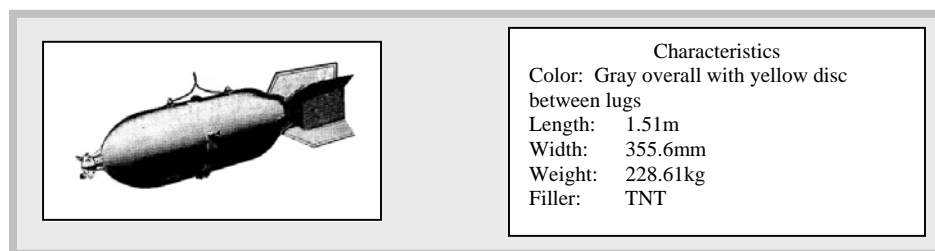
Mines

Similar to the homemade bombs used by terrorists, mines are another means used to inflict damage by terrorist organizations. They use both anti-personnel and anti-tank mines. Unlike conventional military forces that use mines against an opposing military force, terrorists use mines to disrupt social, economic, and political operations. Consequently, mines are often placed around schools, on walking paths, around wells, etc., in order to gain the full terror

effects.[301]   When examining the proliferation of these type weapons throughout the world, it becomes readily apparent that it will be a true threat to U.S. forces. The information in Table F-1 is from the 2001 Landmine Monitor Report and shows the various countries of the world that are affected by landmines and unexploded ordnance. Many of these mines have been emplaced by terrorist organizations.

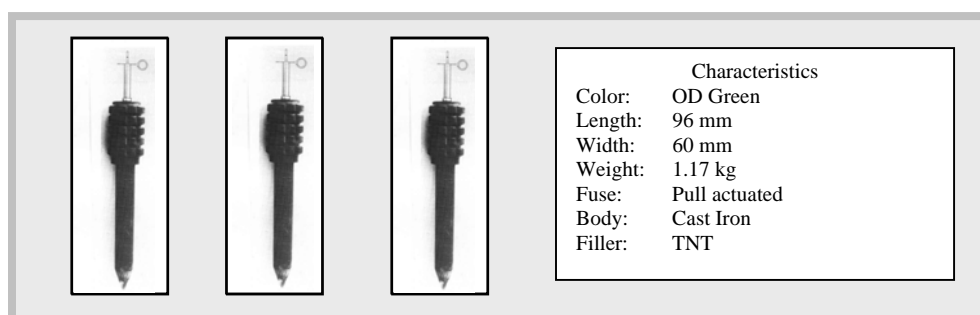| *Africa*	*Americas*	*Asia-Pacific*	*Europe/Central Asia*	*Middle East/North Africa*
Angola	Chile	Afghanistan	Albania	Algeria
Burundi	Colombia	Bangladesh	Armenia	Egypt
Chad	Costa Rica	Burma	Azerbaijan	Iran
Congo-Brazz.	Cuba	Cambodia	Belarus	Iraq
DR Congo	Ecuador	China	Bosnia & Herzegovina	Israel
Djibouti	El Salvador	India	Croatia	Jordan
Eritrea	Guatemala	North Korea	Cyprus	Kuwait
Ethiopia	Honduras	South Korea	Czech Republic	Lebanon
Guinea-Bissau	Nicaragua	Laos	Denmark	Libya
Kenya	Peru	Mongolia	Estonia	Morocco
Liberia	Falkland-Malvinas	Nepal	Georgia	Oman
Malawi		Pakistan	Greece	Syria
Mauritania		Philippines	Kyrgyzstan	Tunisia
Mozambique		Sri Lanka	Latvia	Yemen
Namibia		Thailand	Lithuania	Golan Heights
Niger		Vietnam	FYR Macedonia	Northern Iraq
Rwanda		Taiwan	Moldova	Palestine
Senegal			Poland	Western Sahara
Sierra Leone			Russia	
Somalia			Tajikistan	
Sudan			Turkey	
Swaziland			Ukraine	
Tanzania			Uzbekistan	
Uganda			Yugoslavia	
Zambia			Abkhazia	
Zimbabwe			Chechnya	
Somaliland			Kosovo	
			Nagorno-Karabakh	
Source: "Humanitarian Mine Action", *Landmine Monitor Report – 2001*; available from http://www.icbl.org/lm/2001/exec/hma.html#Heading514; Internet; accessed 13 December 2002.				

Table F-1. Landmine/UXO Problem in the World Today

---

[301] Margaret Buse, "Non-State Actors and Their Significance," *Journal of Mine Action* (December 2002): 2; available from http://maic.jmu.edu/journal/5.3/features/maggie_buse_nsa/maggie_buse.htm; Internet; accessed 13 December 2002.
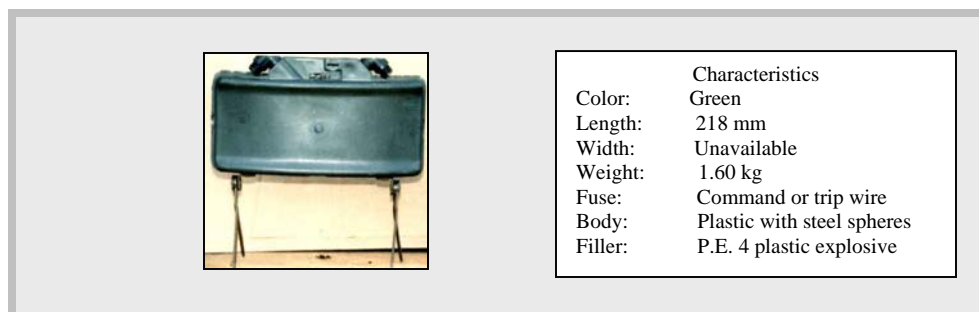
There are hundreds of different types of mines that can be employed against our troops. As Robert Williscroft stated in *Defense Watch*, "At least 800 different mine types populate the world's minefields. These range from homemade coffee can bombs to sophisticated 'smart' non-metallic devices that can distinguish between potential targets."[302] Homemade bombs were discussed in Appendix E on IEDs, so they will not be addressed again. Manufactured mines used by terrorists originate from many of the former Warsaw Pact countries, the United States, China, Britain, and Iran, to name just a few sources.[303] Some common mines are shown below. These can be detonated through the use of trip wires, pressure, or command detonation. These figures are courtesy of the Naval Explosive Ordnance Disposal Technology Division.[304]

- Figure F-22: Chinese (P.R.) Landmine, APERS, Type 59

	Characteristics
Color:	OD Green
Length:	96 mm
Width:	60 mm
Weight:	1.17 kg
Fuse:	Pull actuated
Body:	Cast Iron
Filler:	TNT

- Figure F-23. Chinese (P.R.) Landmine, APERS, Type 66

	Characteristics
Color:	Green
Length:	218 mm
Width:	Unavailable
Weight:	1.60 kg
Fuse:	Command or trip wire
Body:	Plastic with steel spheres
Filler:	P.E. 4 plastic explosive

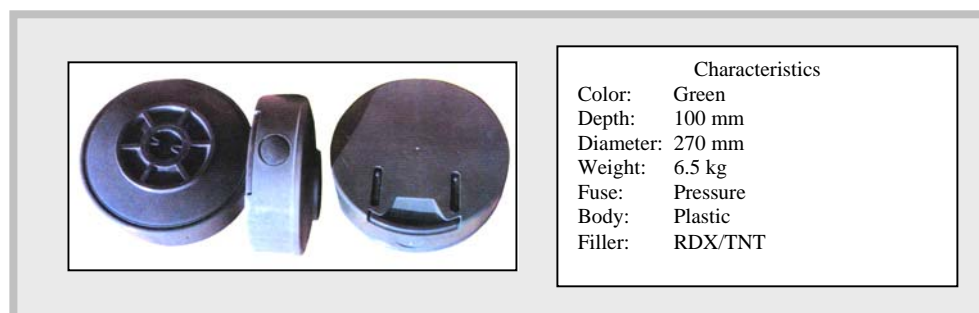[302]Robert G. Williscroft, "The Economics of Demining Defines Success and Failure," *Defense Watch* (13 February 2002): 4; available from http://www.sftt.org/dw02132002.html; Internet; accessed 13 December 2002.

[303] C.J. Clark, *Mine/UXO Assessment: Former Yugoslav Republic of Macedonia* (New York: United Nations Mine Action Coordination Center, 8 October 2001), 2; available from http://www.mineaction.org/sp/mine_awareness/_refdocs.cfm?doc_ID=707; Internet; accessed 13 December 2002; and Jerry White, "Ridding the World of Land Mines," *Union-Tribune* (24 January 2002): 4; available from http://www.wand.org/9-11/discuss6.html; Internet; accessed 13 December 2002.

[304]Department of Defense, Naval Explosive Ordnance Disposal Technology Division, *ORDATA II - Enhanced Deminers' Guide to UXO Identification, Recovery, and Disposal,* Version 1.0, [CD-ROM], (Indian Head, MD: Naval Explosive Ordnance Disposal Technology Division, 1999).

- Figure F-24. Chinese (P.R.) Landmine, AT, Type 72

Characteristics	
Color:	Green
Depth:	100 mm
Diameter:	270 mm
Weight:	6.5 kg
Fuse:	Pressure
Body:	Plastic
Filler:	RDX/TNT

- Figure F-25. U.S. Landmine, APERS, HE, M14

Characteristics	
Color:	Olive drab with black markings
Depth:	38 mm
Diameter:	58 mm
Weight:	85 g
Fuse:	Pressure Activated
Body:	Plastic
Filler:	Tetryl
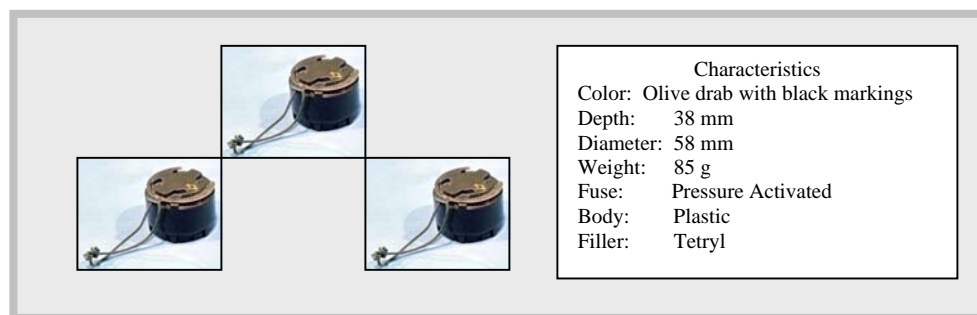
- Figure F-26. U.S. Landmine, APERS, HE, M18A1

Characteristics	
Color:	Olive drab
Length:	216 mm
Width:	83 mm
Weight:	1.6 kg
Fuse:	Tripwire or command detonated
Body:	Plastic with steel ball bearings
Filler:	Composition C4

- Figure F-27. U.S. Landmine, AT, HE, M21

Characteristics
Color: Olive drab with yellow markings
Depth: 114 mm
Diameter: 229 mm
Weight: 8.20 kg
Fuse: Pressure activated
Body: Steel
Filler: Composition B

- Figure F-28. U.S.S.R. Landmine, APERS, Directional, MON-50

Characteristics
Color: Green
Length: 220 mm
Width: 45 mm
Weight: 2 kg
Fuse: Tripwire, break wire, or
command detonated
Body: Plastic with steel ball bearings
Filler: PVV-5A
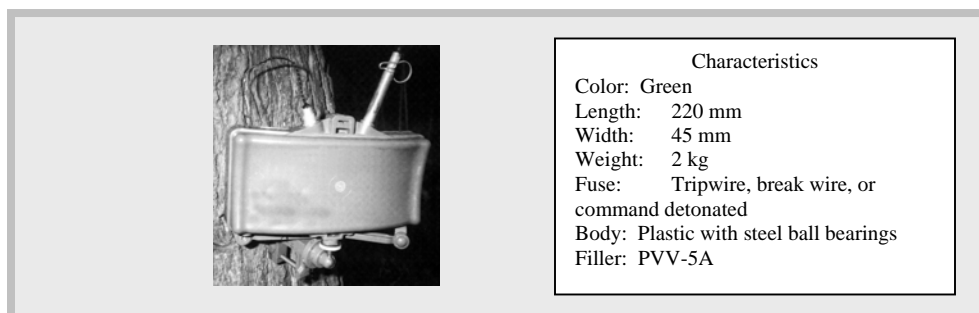
- Figure F-29. U.S.S.R. Landmine, APERS, PMN-2

Characteristics
Color: Green or black
Depth: Unavailable
Diameter: 121.6 mm
Weight: 420 g
Fuse: Pressure activated
Body: Plastic
Filler: TNT – RDX – A1
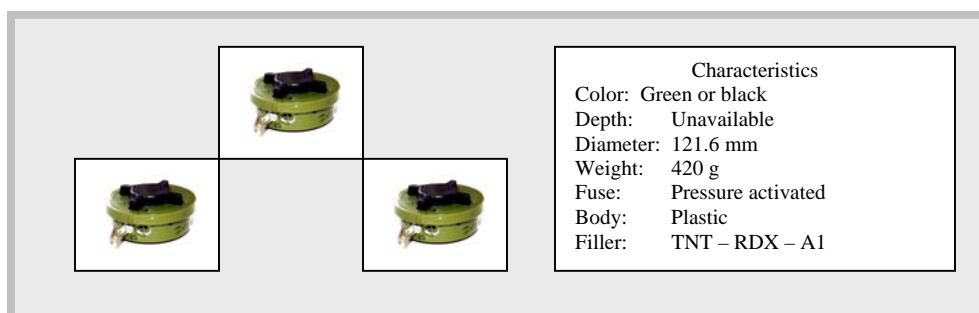
- Figure F-30. U.S.S.R. Landmine, AT, TM-62M

Characteristics
Color: Olive drab/green/brown/khaki/sand
Depth: 102 mm
Diameter: 316 mm
Weight: 8.5 kg
Fuse: Pressure activated
Body: Metal
Filler: Trotyl/Ammonite 80

- Figure F-31. Yugoslav Landmine, APERS, PMA-2

Characteristics
Color: Green with black fuse body
Depth: 62 mm
Diameter: 66 mm
Weight: 133 g
Fuse: Pressure actuated
Body: Plastic
Filler: TNT
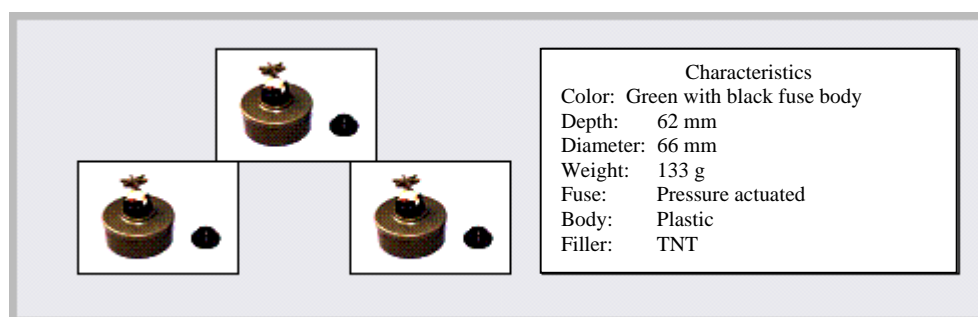
- Figure F-32. Yugoslav Landmine, APERS, PMR-2A

Characteristics
Color: Green
Length: 132 mm
Width: 66 mm
Weight: 1.70 kg
Fuse: Pull actuated
Body: Steel
Filler: TNT
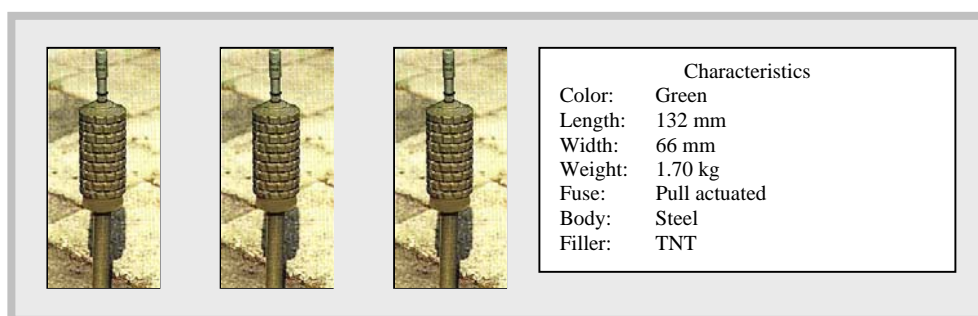
- Figure F-33. Yugoslav Landmine, AT, TMA-4

Characteristics
Color: Light green with yellow markings
Depth: 64 mm
Diameter: 285 mm
Weight: 5.50 kg
Fuse: Pressure actuated
Body: Plastic
Filler: TNT
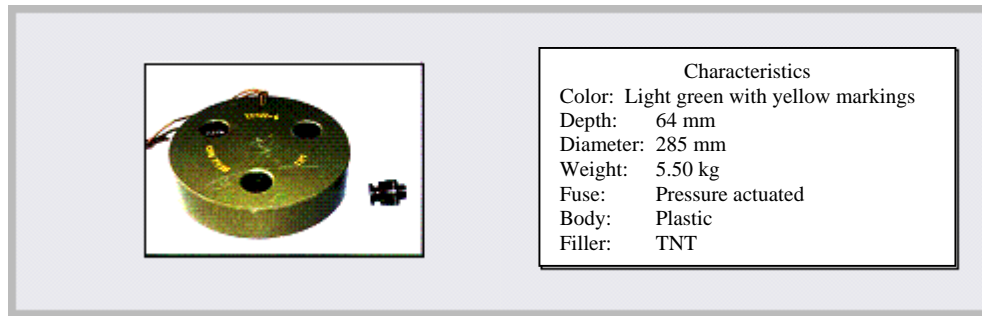
Appendix G
Weapons of Mass Destruction

The future may see a time when such a [nuclear] weapon may be constructed in secret and used suddenly and effectively with devastating power by a willful nation or group against an unsuspecting nation or group of much greater size and material power.

U.S. Secretary of War Henry Stimson to Harry Truman 25 April 1945

General

The specter of weapons of mass destruction (WMD) has existed ever since the term arose in the mid-twentieth century. Actions in World War II witnessed the entry of atomic weapons and their destructive effects, and started a subsequent arms race among nations to obtain and wield such an instrument of power. On closer reflection, other weapons of mass destruction have existed for centuries. Examples include biological vectors used to spread disease among adversaries in ancient and modern periods, or the more recent use of massive chemical weapon attacks in World War I. The acronym "NBC" emerged in the post-World War II era to catalog the main types of mass destruction as nuclear, biological, and chemical weapons.
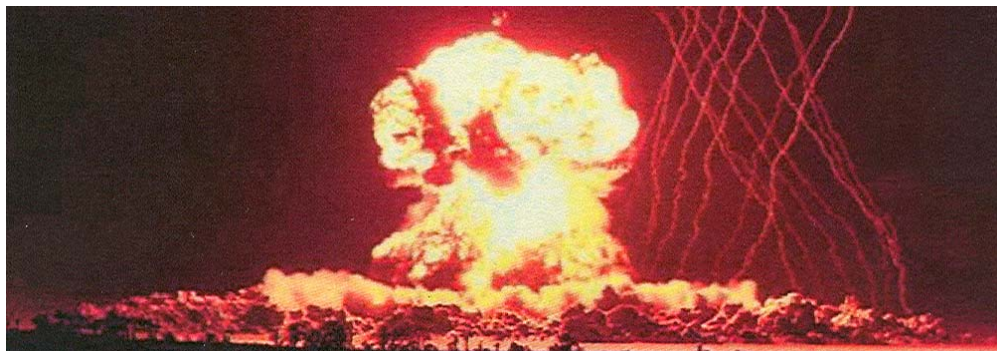
Fig. G-1. **U.S. Nuclear Bomb Detonation**
(*Source:* U.S. Government)

More recently, other means of mass destruction or mass disruption effects entered the lexicon. Radiological weapons, often called radiological dispersal devices (RDD), add to a grouping of weapon capabilities as chemical, biological, radiological, and nuclear (CBRN). High yield explosives can also be considered a weapon of mass destruction. The recognition of explosives with high yield effects now adds a category to weapons of mass destruction and a contemporary acronym of CBRNE.

CBRNE Background

The threat of terrorists using weapons of mass destruction appears to be rising. Incidents since the 1980s spotlight the attention that mass casualties or mass destruction cause in a contemporary setting of near instantaneous global information access. Terrorists quickly realized the value of sensational events that might prompt a change in national policies, alter regional security arrangements, or thrust obscure issues into an international spotlight. The vehicular bombing of the U.S. Embassy in Lebanon in 1983, the World Trade Center in 1993, the U.S. military housing area at Khobar Towers in 1996, the U.S. Embassies in Kenya and Tanzania in 1998, and the aerial attack on the World Trade Center on September 11, 2001 are examples of an escalating notoriety in terrorist assaults. These acts demonstrate the capability and conduct of terrorists to plan, organize, and execute attacks to produce mass casualties.[305] In an unclassified report to the U.S. Congress, the Central Intelligence Agency stated that many of the over 30 designated foreign terrorist organizations have expressed interest in acquiring WMD.[306] Additionally, terrorists state interest in conducting unconventional attacks and make public statements about unconventional weapons.[307] Some terrorists profess that the acquisition of WMD to be a [extremist] religious duty and threaten to use them.[308]

> **"The United States of America is fighting a war against terrorists of global reach. The enemy is not a single political regime or person or religion or ideology. The enemy is terrorism – premeditated, politically motivated violence perpetrated against innocents."**
>
> National Security Strategy of the United Sates of America

Terrorist groups that acquire CBRNE weapons pose a critical danger. Terrorists armed with these weapons can gain leverage for their demands by threatening use of these weapons to influence political or military actions or to achieve a specific economic or financial objective. Likewise, some groups simply want to employ WMD to create large numbers of casualties, both military and civilian, and capitalize on the effects of these events.[309]

In a May 1998 interview, Usama bin Laden stated, "We do not have to differentiate between military or civilian. As far as we are concerned, they are all targets, and this is what the fatwa

---

[305] Department of State, *Patterns of Global Terrorism 2001* (Washington, D.C., May 2002), 66.

[306] Director of Central Intelligence, DCI Weapons Intelligence, Nonproliferation, and Arms Control Center, *Unclassified Report to Congress on the Acquisition of Technology Realting to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2003* (Washington, D.C., January 2002), 7; available from http://www.cia.gov/cia/reports/721_reports/pdfs/jan_jun2003.pdf; Internet; accessed 19 May 2004.

[307] Ibib., 8-9.

[308] Department of State, *Patterns of Global Terrorism 2001* (Washington, D.C., May 2002), 66.

[309] The White House, National Security Presidential Directive 17 (NSPD-17), *National Strategy to Combat Weapons of Mass Destruction*, (Washington, D.C., December 2002), 4 and 10; available from http://www.fas.org/irp/offdocs/nspd/nspd-17.html; Internet; accessed 8 December 2003.

says."[310] Additionally, al Qaeda spokesman Suleiman abu Ghaith has stated: "We have the right to kill four million Americans – two million of them children – and to exile twice as many and injure and cripple hundreds of thousands. We have the right to fight them by chemical and biological weapons, so they catch the fatal and unusual diseases that Muslims have caught due to their [U.S.] chemical and biological weapons."[311] These statements by al Qaeda leave no doubt that some terrorists are committed to using weapons of mass destruction if they can acquire them. In the Cold War era of earlier decades in the twentieth century, weapons of mass destruction were considered weapons of last resort and threatened mutual devastation among super-powers. Today, some terrorists see weapons of mass destruction as weapons of choice.[312]

> **"Acquiring weapons for the defense of Muslims is a religious duty. If I have indeed acquired these weapons (WMD), then I thank God for enabling me to do so. And if I seek to acquire these weapons, I am carrying out a duty. It would be a sin for Muslims not to try to possess the weapons that would prevent the infidels from inflicting harm on Muslims."**
>
> Usama Bin Laden interview with *Time Magazine*, December 23, 1998

Weapons of Mass Destruction Categories

Weapons of mass destruction are normally classified into five categories: chemical, biological, radiological, nuclear, and high yield explosives.

> **"Rogue states and terrorists do not seek to attack us using conventional means. They know such attacks would fail. Instead, they rely on acts of terror and, potentially, the use of weapons of mass destruction – weapons that can be easily concealed, delivered covertly, and used without warning."**
>
> National Security Strategy of the United Sates of America

---

[310] Ben N. Venzke and Aimee Ibrahim, *al Qaeda Tactic/Target Brief*, Version 1.5 (Alexandria, VA: IntelCenter, 2002), 8.

[311] Ibid., 10.

[312] National Security Strategy of the United States of America, 8.

Chemical Weapons

The range of chemical weapons contains substances intended to kill or incapacitate personnel and to deny use of areas, materiel, or facilities. Agents can be both lethal and non-lethal, and can be either persistent or nonpersistent. As with biological weapons, terrorists have already exhibited the capability to use chemical weapons. One example was demonstrated in 1978 when a group of Palestinians injected oranges with cyanide to damage Israel's citrus exports.[313] Additionally, in 1995 the Japanese cult Aum Shinrikyo released sarin nerve agent in the Tokyo subway network killing 12 people and injuring 5,500.[314] The Aum Shinrikyo attack shows the unpredictable nature of chemical weapons and problematic issues of dissemination. This Japanese cult was able to produce and release sarin in a closed environment, but fortunately, the effects were much less deadly than planned by the terrorists.

The aerial attacks on September 11, 2001 by suicidal aircraft raised the chemical industry's awareness of possible terrorist sabotage of facilities that store toxic industrial chemicals. These type attacks could provide the mass casualty effects of a chemical weapons attack, yet would not present the terrorist group with the problem of developing or acquiring chemical agents. A tragic scenario occurred in Bhopal, India in 1984 when a disgruntled pesticide plant employee is believed to have released 40 metric tons of methyl isocyonate into the atmosphere. The resulting casualties were 2,000 local residents killed and 100,000 injured people.[315]

Chemical agents are categorized by the effects they have on the target population. Lethal agents include nerve, blood, blister, and choking agents. Nonlethal agents include incapacitants and irritants.

Table G-1 lists characteristic effects of various chemical agents.

Agent	*Lethal*	*Symbol Name*	*Symptoms in Man*	*Effects on Man*	*Rate of Action*
Nerve	Yes	G Series GB/Sarin GD/Soman (VR 55)	Difficult breathing, sweating, drooling, nausea, vomiting convulsions, and dim or blurred vision.	At low concentrations, incapacitates; Kills if inhaled or absorbed through The skin.	Very rapid by inhalation; slower through skin (5-10 minutes).
	Yes	V Agent	Same as above.	Incapacitates; kills if skin is not rapidly decontaminated	Delayed through skin; more rapid through eyes.

---

[313] *Encyclopedia of World Terrorism*, 1997 ed., s.v. "Chemical."

[314] Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999), 54.

[315] Steve Bowman, *Weapons of Mass Destruction: The Terrorist Threat* (Washington, D.C.: Congressional Research Service Report for Congress, 7 March 2002), 7; available from http://www.fas.org/irp/crs/RL31332.pdf; Internet; accessed 23 December 2002.

Blood	Yes	AC/Hydrogen cyanide	Rapid breathing, convulsions, coma, and death.	Incapacitates; kills if high concentration is inhaled.	Rapid
Blister	Yes	HD/Mustard HN/Nitrogen Mustard L/Lewisite HL/Mustard and Lewisite CX/Phosgene Oxime	Mustard, nitrogen mustard: no early symptoms. Lewisite and mustard: searing eyes and stinging skin. Phosgene oxime: powerful irritation of eyes, nose, and skin.	Blisters skin and respiratory tract; can cause temporary blindness. Some agents sting and form wheals on skin.	Blister delayed hours to days; eye effects more rapid.
Choking	Yes	CG/Phosgene DP/Diphosgene	Eye-throat irritation, fatigue, tears, cough, chest tightness, nausea, vomiting.	Damages the lungs.	Delayed, variable.
Incapaci-tant	No	BZ	Slowing of mental and physical activity, disorientation/sleep.	Temporarily incapacitates.	30-60 minutes.
Irritant	No	DA/Diphenyl-chloroarsine DM/Adamsite CN/Chloro-acetophenone CS/O-Chloro-benzylidene-malononitrile PS/Chloropicrin	Causes tears, irritates skin and respiratory tract.	Incapacitates, non-lethal.	Very rapid.

Table G-1. Effects of Example Chemical Agents.

Nerve agents are fast-acting chemical agents. Practically odorless and colorless, they attack the body's nervous system causing convulsions and eventually death. Nerve agents are further classified as either G or V agents.

At low concentrations, the GB series incapacitates; it kills if inhaled or absorbed through the skin. The rate of action is very rapid if inhaled, but slower if absorbed through the skin. The V-agents are quicker acting and more persistent than the G-agents.

Blood agents are absorbed by breathing and block the oxygen transferal mechanisms in the body, leading to death by suffocation. A common blood agent is hydrogen cyanide. It kills quickly and dissipates rapidly.

Blister agents, such as mustard (H) or lewisite (L), and combinations of the two compounds, can disable or kill. These type agents burn the skin and produce large blisters. They also cause damage to the eyes, blood cells, and lungs. These agents are especially harmful when inhaled.

Choking agents, such as phosgene and diphosgene, attack the respiratory system and make the membranes swell so the lungs fill with fluid, which can be fatal. As with blood agents, poisoning from choking agents comes through inhalation, since both types of agents are nonpersistent. Signs and symptoms of toxicity may be delayed up to 24 hours.

Incapacitants include psychochemical agents and paralyzants. These agents can disrupt a victim's mental and physical capabilities. The victim may not lose consciousness, and the effects usually wear off without leaving permanent physical injuries.

Irritants, also known as riot-control agents, cause a strong burning sensation in the eyes, mouth, skin, and respiratory tract. The effects of these agents, the most commonly known being "tear gas" (CS), are also temporary. Victims recover without having any serious aftereffects.

Chemical agents are also classified according to their persistency. Persistency is the length of time an agent remains effective on the battlefield or other target area after dissemination. The two basic classifications are persistent or nonpersistent.

Persistent nerve agents, such as V-agents, thickened G-agents, and the blister agent mustard, can retain their disabling or lethal characteristics for days to weeks (depending on environmental conditions). Persistent agents produce either immediate or delayed casualties. Immediate casualties occur when an individual inhales a chemical vapor. Delayed casualties occur when the chemical agent is absorbed through the skin, thus demonstrating the need for protective equipment.

Fig. G-2. **Chemical Protection**
(*Source:* U.S. Army Photo)

Nonpersistent agents generally last a shorter period of time, depending on the weather conditions. For example, the nerve agent sarin (GB) forms clouds that dissipate within minutes after dissemination. However, some liquid GB could remain for periods of time varying from hours to days, depending on the weather conditions and method of delivery.

Dissemination is a significant difficulty in using chemical weapons and achieving the desired weapon effects. Vapors are affected by the direction of the wind as well as temperature. Additionally, there are biological activities that diminish the toxicity of the agent, therefore, the amount of chemical needed in the open air or in water to have its intended effect is much larger than what is successful in the laboratory.[316]

Numerous means to include mortars and bombs can be used to deliver chemical warfare agents. Chemical munitions are fitted with different burst capabilities, according to the agent properties and the intended effect. For example, a chemical munitions fitted with a long burst fuse releases the agent as a vapor or fine aerosol. This creates an immediate inhalation hazard with some of the fragmentation effect of conventional munitions. Theoretically, terrorists could obtain these munitions, modify them and emplace them by hand. Delivery means could be by vehicle, backpack, canisters or sprayers, similar to those used for biological agents. Another means could be the misuse of toxic industrial chemicals in massive quantities.

---

[316]Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999), 60.

Toxic Industrial Chemicals

There is a near-universal availability of large quantities of highly toxic stored materials. Exposure to some industrial chemicals can have a lethal or debilitating effect on humans, which, in combination with their ready availability, their proximity to urban areas, their low cost, and the low security associated with storage facilities, makes them an attractive option for terrorist use as weapons of opportunity or of mass destruction.

The most important factors to consider when assessing the potential for adverse human health impacts from a chemical release are acute toxicity, physical properties (volatility, reactivity, flammability), and likelihood that large quantities will be available for exploitation. Foremost among these factors is acute toxicity; thus, the highest concern for human health is associated with a subgroup of industrial chemicals known as toxic industrial chemicals (TICs). TICs are commercial chemical substances with acute toxicity that are produced in large quantities for industrial purposes. Knowledge of where these type chemicals are stored and how they are transported are only two of many factors in assessing possible terrorist use.

Table G-2 lists high- and moderate-risk TICs based on acute toxicity by inhalation, worldwide availability (number of producers and number of continents on which the substance is available), and physical state (gas, liquid, or solid) at standard temperature and pressure.

High Risk	*Moderate Risk*	
Ammonia	Acetone cyanohydrin	Methyl chloroformate
Arsine	Acrolein	Methyl chlorosilane
Boron trichloride	Acrylonitarile	Methyl hydrazine
Boron trifluoride	Allyl alcohol	Methyl isocyanate
Carbon disulfide	Allyl amine	Methyl mercaptan
Chlorine	Allyl chlorocarbonate	n-Butyl isocyanate
Diborane	Boron tribromide	Nitrogen dioxide
Ethylene oxide	Carbon monoxide	Phosphine
Fluorine	Carbonyl sulfide	Phosphorus oxychloride
Formaldehyde	Chloroacetone	Phosphorus pentafluoride
Hydrogen bromide	Chloroacetonitrile	Selenium hexafluoride
Hydrogen chloride	Chlorosulfonic acid	Silicon tetrafluoride
Hydrogen cyanide	Crotonaldehyde	Stibine
Hydrogen fluoride	Diketene	Sulfur trioxide
Hydrogen sulfide	1,2-Dimethyl hydrazine	Sulfuryl chloride
Nitric acid, fuming	Dimethyl sulfate	Tellurium hexafluoride
Phosgene	Ethylene dibromide	Tert-Octyl mercaptan
Phosphorus trichloride	Hydrogen selenide	Titanium tetrachloride
Sulfur dioxide	Iron pentacarbonyl	Trichloroacetyl chloride
Sulfuric acid	Methanesulfonyl chloride	Trifluoroacetyl chloride
Tungsten hexafluoride	Methyl bromide	

Table G-2. High- and Moderate-Risk Toxic Industrial Chemicals

Some chemicals in solid form need only to be exposed to air or water in order to turn into a toxic gas. In addition, the current definition of TICs does not include all chemicals with high toxicity and availability. Specifically, chemicals with low volatility are not included. These low-vapor-pressure chemicals include some of the most highly toxic chemicals widely available, including most pesticides.

Biological Weapons

Biological weapons consist of pathogenic microbes, toxins, and bioregulator compounds. Depending on the specific type, these weapons can incapacitate or kill people and animals; and destroy plants, food supplies, or materiel. The type of targets being attacked determines the choice of agents and dissemination systems.

Biological warfare agents are virtually undetectable while they are in transit and evidence of a biological attack may not show up for days after the actual release has occurred. These agents are easier and cheaper to produce than either chemical or nuclear weapons, and the technology is readily available on the Internet. In fact, any nation with a modestly sophisticated pharmaceutical industry is capable of producing these type agents.[317] Biological agents are also very lethal. Whereas about 1800 pounds of sarin is required to inflict a large number of casualties over a square mile area, under ideal conditions, only a quarter ounce of anthrax spores is required to achieve the same effect.[318]

The Fall 2001 anthrax attacks in the United States following the World Trade Center and Pentagon bombings show that terrorists will use biological weapons. Although the anthrax attacks were originally suspected to be linked to al Qaeda or Iraq, there is no evidence that a known terrorist organization was involved. Current views indicate that the attacks were probably domestically initiated or that a lone terrorist with previous access to weapon quality anthrax conducted them.[319] Although the outcome of these attacks resulted in few casualties, the attacks did show the psychological and economic disruption such attacks could cause. Washington, D.C. and other East Coast cities were in a panic dealing with these attacks. Additionally, the numerous hoaxes using talcum powder showed the psychological and economic impact of the potential use of these type weapons.

Although the anthrax attacks from 2001 achieved recognizable publicity, biological attacks in the United States are not new. Biological terrorism occurred in Oregon in 1984 with food tampering. Followers of the Bagwan Shree Rajneessh cult placed salmonella on salad bar food in several restaurants, causing over 700 people to become ill.[320]

---

[317] Canadian Security Intelligence Service, "Report 2000/05 Biological Weapons Proliferation," *Perspectives* (9 June 2000): 2; available from http://www.csis-scrs.gc.ca/eng/miscdocs/200005_e.html; Internet; accessed 6 February 2003.

[318] *Encyclopedia of World Terrorism*, 1997 ed., s.v. "Biological."

[319] Steve Bowman, *Weapons of Mass Destruction: The Terrorist Threat* (Washington, D.C.: Congressional Research Service Report for Congress, 7 March 2002), 3; available from http://www.fas.org/irp/crs/RL31332.pdf; Internet; accessed 23 December 2002.

[320] Department of Justice, Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, Counterterrorism Division, *Terrorism in the United States 1999,* Report 0308, (Washington, D.C., n.d.), 39.

Biological warfare agents include three basic categories: pathogens, toxins, and bioregulators. Table G-3 lists some examples of each.

Pathogens	Toxins	Bioregulators
Anthrax	Mycotoxins	Neurotransmitters
Cholera	Venoms	Hormones
Plague	Shell fish	Enzymes
Smallpox	Botulinum	
Tularemia	Ricin	
Influenza		
Fevers		

Table G-3. Examples of Biological Warfare Agents

Some of the characteristics of biological weapons are shown below[321]:

Agent	Contagious	Mortality if Untreated	Incubation Period (Days)	Illness Duration (Days)
Anthrax	No	90-100%	1-7	3-5
Plague	Yes	100%	1-6	Fatal within 6
Tularemia	No	30-40%	1-14	14 or more
Smallpox	Yes	30%	7-17	10-28
Botulinum	No	60-100%	1-5	Days to weeks
Ricin	No	Variable	18-24 hours	Days

Table G-4. Characteristics of Biological Weapons

Pathogens cause diseases such as anthrax, cholera, plague, smallpox, tularemia, or various types of fever. These weapons could be used against targets such as food supplies, port facilities, and population centers. Of particular concern is the threat of contagious diseases, such as smallpox. Since it has an incubation period that can last over 2 weeks without any symptoms, the release of smallpox could easily infect a large number of people in a short period of time.

Living organisms, such as snakes, spiders, sea creatures, and plants, produce toxins. Toxins are faster acting and more stable than live pathogens. Most toxins are easily produced through genetic engineering.

Fig. G-3. **Man with Smallpox**
(Source: CDC/Barbra Rice)

Bioregulators are chemical compounds that are essential for the normal psychological and physiological functions. A wide variety of bioregulators are normally present in the human

---

[321]Lewis M. Simons, "Weapons of Mass Destruction: An Ominous New Chapter Opens on the Twentieth Century's Ugliest Legacy," *National Geographic* 202, no. 5 (November 2002): 22-23.

body in extremely minute concentrations. These compounds can produce a wide range of harmful effects if introduced into the body at higher than normal concentrations or if they have been altered. Psychological effects could include exaggerated fear and pain. In addition, bioregulators can cause severe physiological effects such as rapid unconsciousness, and, depending on such factors as dose and route of administration, they could also be lethal. Unlike pathogens that take hours or days to act, bioregulators could act in only minutes.

Another way to categorize biological warfare agents is by their effects. The four categories and effects of biological agents are shown in Table G-5. There is a threat of agro-terrorism, which affects plants and animals. The outbreaks of foot-and-mouth disease and mad cow disease in Europe and the isolated case of mad cow in the U.S. state of Washington[322] are recent examples of the economic impact of such diseases. Additionally, this type terrorism allows a terrorist group to inflict significant economic and social disruption without the stigma of inflicting large numbers of human casualties.[323] Based on statements from al Qaeda that they intend to target key sectors of the U.S. economy, agro-terrorism is a likely threat.

Agent Type	Agent Effects
Antipersonnel	Disease or death causing microorganisms and toxins
Antiplant	Living micro-organisms that cause disease or death
Antianimal	Agents that can be used to incapacitate or destroy domestic animals through disease. Used to limit wool, hide, or fur production.
Antimaterial	Agents used to deteriorate critical materiel needed for the war effort such as leather, canvas, fuels, or electronics.

Table G-5. Effects of Biological Agents

Biological dissemination through aerosols, either as droplets from liquid or as particles from powders, is the most efficient method. This method does create a challenge since aerosol disseminators need to be properly designed for the agent used, and proper meteorological conditions must exist to conduct an effective attack.[324] The objective of biological weapon delivery is to expose humans to an agent in the form of a suspended cloud of very fine agent particles. Airborne particles, once inhaled, tend to lodge deep in the lungs close to vulnerable body tissues and the bloodstream.

Terrorists can deliver biological weapons by unconventional dissemination means. These include commercially available or specially designed sprayers or other forms of aerosol generators mounted in automobiles, trucks, or ships. Smaller, more portable devices could be used to effectively disseminate biological agent aerosols. Such devices could be used to introduce an agent into heating, ventilating, and air conditioning systems. Drinking water can be contaminated by means of high-pressure agent injectors attached to plumbing system components. Insects, rodents, or other arthropod vectors are other feasible

---

[322] "Final BSE Update – Monday, February 9, 2004," USDA United States Department of Agriculture website; available from http://usda.gov/Newsroom/0074.04.html; Internet; accessed 12 July 2004.

[323] Steve Bowman, *Weapons of Mass Destruction: The Terrorist Threat* (Washington, D.C.: Congressional Research Service Report for Congress, 7 March 2002), 6; available from http://www.fas.org/irp/crs/RL31332.pdf; Internet; accessed 23 December 2002.

[324] Steve Bowman, *Weapons of Mass Destruction: The Terrorist Threat*, 5.

vectors of dissemination. Methods of dissemination are varied and limited only by the terrorist imagination.

Radiological Weapons

Radiological terrorism, a relatively new aspect of WMD and terrorism, is usually conceived as the horrific use of a radiological device or an attack on a nuclear facility such as a nuclear power plant.

Radioactivity is the release of energy in the form of radiation, as some naturally occurring elements attempt to change their fundamental atomic structure. Isotopes are forms of these particular elements that have distinct nuclear properties. When an isotope is unstable, it emits radiation and is called a radioisotope. Radiation from radioisotopes can damage human cells and cause problematic health issues.[325]

Although physical destruction with a radiological device may be much less than a nuclear detonation, radiological contamination, or the fear of radiation on long-term health issues, may be a key psychological impact. Physical and psychological trauma of a radiological threat can have significant negative effects on the economic, financial, and political programs of a region and nation.

Radiological contamination can occur in multiple ways. One of the more well-known dissemination descriptions is a radiological dispersal device (RDD). This capability uses any number of mechanical means to spread radiation throughout a designated area. Another common term, "dirty bomb," is an example of using conventional explosives to disperse radioactive material. Other forms of RDD could distribute radioactive material in the atmosphere or in confined areas such as an office complex ventilation system. A passive method of radiological attack could be the use of a radiation-emitting device (RED). In this example, a RED could be positioned to expose a population to intense radiation for a short period of time, or expose a selected population to low radiation over an extended period. The knowledge of contamination, and the fear of physical or psychological harm could be significant.[326]

> **"When 100 years ago authorities had to worry about the anarchist placing a bomb in the downtown square…now we must worry about the terrorist who places the bomb in the square, but packed with radiological material."**
>
> Spencer Abraham, U.S. Secretary of Energy 2003

---

[325] ""Chemistry 101": The Make-up and Importance of Radioisotopes," *Introduction to Radiological Terrorism,* 1; available from http://www.nti.org/h_learnmore/radtutorial/chapter01_03.html; Internet; accessed 19 May 2004.

[326] "What is Radiological Terrorism?" *Introduction to Radiological Terrorism,* 1 and 2; available from http://www.nti.org/h_learnmore/radtutorial/chapter01_02.html; Internet; accessed 19 May 2004.

The many industrial, scientific, agricultural, and public arena uses of radiation make access to certain radiological equipment and materiel a distinct probability for a dedicated individual or group. The 1995 demonstration of Chechnyan rebels burying a container of radioactive material in a Moscow public park received international attention. Not as well known is a 1999 incident of thieves in Grozny, Chechnya attempting to steal a container of radioactive material from a chemical factory. One thief died almost immediately after exposure to the container, and an accomplice was hospitalized in serious condition.[327] As an additional example of radioactive material, the former Soviet Union employed highly radioactive thermoelectric generators (RTG) to remotely power naval navigational systems and other military facilities.[328] In one 2001 incident report, two people scavenging for lead in a Russian facility were hospitalized after dangerous exposure to radioactive material. In a 2001 report from the nation of Georgia, individuals received significant radiation contamination after they handled abandoned containers holding a radioactive substance. In 2003, a report notes that police in the nation of Georgia discovered radioactive containers and other materials in a routine vehicle search.

Although radiation type devices may not necessarily cause mass casualties, they could present a significant radiation contamination effect on the target area.[329] Radiation casualties could be low initially, but would potentially increase over time. However, just the fact that a "nuclear" type weapon was employed would have a significant psychological impact on the populace where it is detonated or used. The U.S. Environmental Protection Agency (EPA) guidelines recommend that if a cancer risk due to remaining radiation cannot be reduced to less than one person per 10,000 people, the area should be abandoned. Disaster response and recovery issues of decontamination would include medical treatment of people in the affected area, possible evacuation or relocation of populations, and multiple actions to make physical property and materiel useable with no fear of radiation.[330]

Instances of acquiring materiel to build radiological devices can be very easy with basic knowledge of processes and a dedicated action plan. One example in 1994 is the attempt by a U.S. citizen to build a breeder reactor in his mother's garden shed. This incident had nothing to do with terrorism but does highlight risk, and at the time, the relative ease of obtaining radioactive material. As a teenager, David Hahn used his knowledge of chemistry, inquisitive mind, false documents and statements, and false cover stories to acquire radiological material. He constructed a crude radiological device that could have endangered 40,000 local residents. Questioned by local police for an unrelated citizen complaint, the unexpected discovery of radioactive material triggered the Federal Radiological Emergency Response Plan.[331]

---

[327] "History of Radiological Terrorism," *Introduction to Radiological Terrorism,* 1 to 3; available from http://www.nti.org/h_learnmore/radtutorial/chapter03_01.html; Internet; accessed 19 May 2004.
[328] "Medical Uses," *Introduction to Radiological Terrorism,* 3; available from http://www.nti.org/h_learnmore/radtutorial/chapter01_05.html; Internet; accessed 19 May 2004.
[329] Steve Bowman, *Weapons of Mass Destruction: The Terrorist Threat* (Washington, D.C.: Congressional Research Service Report for Congress, 7 March 2002), 4; available from http://www.fas.org/irp/crs/RL31332.pdf; Internet; accessed 23 December 2002.
[330] "Economic Effects," *Introduction to Radiological Terrorism,* 1; available from http://www.nti.org/h_learnmore/radtutorial/chapter02_02.html; Internet; accessed 19 May 2004.
[331] Ken Silverstein, "David Hahn, Boy Atomic Scientist," *ASEPCO*, [Originally printed in *Harpers's Magazine*, November 1998]; available from http://www.asepco.com/David_Hahn_Boy_Scientist.htm; Internet; accessed 31 August 2004.

To date, the U.S. has not been attacked with a radiological weapon by terrorists. Nonetheless, theoretical case study examples illustrate the potential impacts of a radiological "dirty bomb." In testimony before the U.S. Senate Foreign Relations Committee, illustrations and degrees of contamination were estimated on several factors.[332] These model assumptions included amount of material released, the specific radiological material, dispersal technique, wind speed and direction and other weather conditions, size of particles released into the wind, and types of urban building construction and urban pattern of populations. Complex models have inherent uncertainties in predictive results, however, one example assumed a conventional explosion that dispersed radiological contamination in dust-like particles capable of being inhaled. Dust settling in the affected area, as well as contaminated food or water sources, could be vectors of potential radiation exposure. Any real incident of radiological contamination would cause significant disruption of social, medical, economic, fiscal, and governmental operations, compounded with overarching psychological trauma.

Attack on a nuclear facility is another means to cause radiological contamination. Even with the redundant safeguards and security measures at nuclear facility locations, the possibility of terrorist assault and breach of these measures is not impossible. Yet, considerable precautions and security measures are in effect to preclude successful attacks by vehicle borne explosive devices or aerial borne means. Although remote in expectation, the possibility of a member of a nuclear facility workforce negating facility safeguards and assisting a terrorist act receives constant review and evaluation.[333]

Although the 1986 Chernobyl accident at a nuclear power station in the Ukraine had no connection to terrorism, the resulting political, financial, and social impacts are profound and provide an illustration of what damage radiological contamination can cause. An 18-mile radius around the nuclear plant was closed to everyone except official teams, the large local city near the site was completely evacuated and abandoned, and between 400,000 people[334] and 130,000[335] people were resettled to safe areas. Reports note that over 20 towns and 3000 settlements were affected by radiation doses of significance. Over 400 settlements had to be evacuated.[336] Over 30 people died from the accident while long-term effects on a regional population remain an open-ended issue. Health, economic, and agricultural impacts are still being assessed as various international programs deal with safety, decontamination, and stabilization of equipment, facilities, and the region at a growing cost in the hundreds of millions of dollars.[337]

---

[332] "Dirty Bombs: Response to a Threat," FAS Public Interest Report, *The Journal of the Federation of American Scientists* vol 55 no2 (March/April 2002), 1-11; available from
http://ww.fas.org/faspir/2002/v55n2/dirtybomb.htm; Internet; accessed 15 April 2004.
[333] "Terrorists and Radiological Terrorism," *Introduction to Radiological Terrorism,* 2 and 3; available from
http://www.nti.org/h_learnmore/radtutorial/chapter04_02.html; Internet; accessed 19 May 2004.
[334] "History of the United Nations and Chernobyl," The United Nations and Chernobyl, 1; available from
http://www.un.org/ha/Chernobyl; Internet; accessed 1 July 2004.
[335] "Fact Sheet on the Accident at the Chernobyl Nuclear Power Plant," U.S. Nuclear Regulatory Commission, 1
to 4; available from http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fschernobyl.html; Internet;
accessed 1 July 2004.
[336] "History of the Chernobyl disaster,' 1 and 2; available from http://www.Chernobyl.org.uk/page 2.htm;
Internet; accessed 30 June 2004.
[337] "Fact Sheet on the Accident at the Chernobyl Nuclear Power Plant," U.S. Nuclear Regulatory Commission, 1
to 4; available from http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fschernobyl.html; Internet;
accessed 1 July 2004.

The 1979 accident at Three Mile Island (TMI-2) is the most serious nuclear power plant accident in the United States to date. No terrorism was involved in this accident, but the incident highlights the potential for radiological disaster and psychological impact on a regional population. The plant experienced a partial core meltdown that could have breached the containment building and dispersed massive quantities of radiation into the environment. Fortunately, this breach did not occur, even though a significant amount of radiation was released into the atmosphere. No death or injury occurred to plant workers or citizens of nearby communities during the

Fig. G-4.. **U.S. Nuclear Plant**
(*Source:* U.S Government)

Three Mile Island accident. Multiple government and independent studies conclude that most of the radiation was contained and what radiation was released caused negligible effects on the physical health of individuals or the environment. Nonetheless, the safety and cleanup operations have spanned decades with a corresponding major fiscal cost. [338]

Nuclear Weapons

The use of a fully developed nuclear weapon is a possible attack scenario but would require extraordinary terrorist financial and technical resources. A more likely scenario deals with nuclear material and sabotage or a siege-hostage situation at a nuclear facility.[339] This type scenario aligns more correctly with a radiological incident. Nonetheless, the potential effects could be catastrophic to a surrounding area and population.

Some groups may have state sponsors that possess or can obtain nuclear weapons, but the CIA has no credible reporting at this time of terrorists successfully acquiring nuclear weapons or sufficient material to make them.[340] However, since the collapse of the Soviet Union in 1989, there has been a growth in nuclear trafficking. It's believed that three shipments of Plutonium 239 intercepted by the German police in 1994 came from Russia.[341] Since 1991, Russian authorities say there have been 23 attempts to steal fissile material, some of which have been successful. Intelligence officials believe enough nuclear material has left Russia to make a bomb.[342] Table G-6 reflects the general quantities of material required to build a crude atomic bomb.[343] As demonstrated in al Qaeda statements, when and if a terrorist group does obtain a nuclear weapon, attack with a WMD is a distinct possibility.

---

[338] "Fact Sheet on the Accident at Three Mile Island," U.S. Nuclear Regulatory Commission, 1 to 5; available from http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle,html; Internet; accessed 1 July 2004.
[339] *Encyclopedia of World Terrorism*, 1997 ed., s.v. "Nuclear."
[340] Director of Central Intelligence, DCI Weapons Intelligence, Nonproliferation, and Arms Control Center, *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2001* (Washington, D.C., January 2002), 9.
[341] *Encyclopedia of World Terrorism*, 1997 ed., s.v. "Nuclear."
[342] Lewis M. Simons, "Weapons of Mass Destruction: An Ominous New Chapter Opens on the Twentieth Century's Ugliest Legacy," *National Geographic* 202, no. 5 (November 2002): 16.
[343] *Weapons of Mass Destruction* (New York: United Nations Office on Drugs and Crime, December 2002), 6; available from http://www.undcp.org/odccp/terrorism_weapons_mass_destruction_page006.html; Internet; accessed 19 December 2002.

Type Fissile Material	Required for a Weapon
Plutonium (Pu)	7 kg
Plutonium oxide (PuO2)	10 kg
Metallic uranium (U-235)	25 kg
Highly enriched uranium oxide (UO2)	35 kg
Intermediate enriched uranium oxide (UO2)	200 kg

Table G-6. Fissile Material

The size of most nuclear weapons makes them hard to clandestinely transport. Backpacks and images of "suitcase" nuclear bombs convey the concept of covertly delivering small nuclear weapons or dangerous radiological dispersion devices. The most likely means of transporting them would be via commercial shipping, such as trucks, vehicles, and ships.[344]

High Yield Explosives

High yield explosives are another significant threat for weapon effects of mass destruction or mass disruption. Terrorist targeting includes critical infrastructure and key assets, and can also aim at causing mass casualties. Terrorists are relentless and patient; they will seize on opportunity and can demonstrate flexibility in strategy and tactics. Attack may occur against a critical node, system, or function. Beyond the physical damage or destruction, attack may cause a cascading disruption for government, social order, and economics as the public and private sectors react. Intent may focus on damage to national prestige, morale, or confidence, as well as legitimate concerns of public health and safety.[345] An attack can also be exploited to assist in near-simultaneous or follow-on assault against separate targets.

Acts of terrorism using high yield explosives have been conducted by foreign and domestic terrorists against the United States. The incidents of the foreign terrorist bombing of the U.S. Embassy and Marine Barracks in Lebanon in 1983 and the domestic terrorist bombing of the Murrah Federal Building in Oklahoma City, Oklahoma in 1995 are well known examples.

In April 1983, a truck loaded with about 400 pounds of explosives rammed into the U.S. Embassy in Beirut, Lebanon. This suicidal attack killed 63 people, including 17 Americans.[346] Eight members were employees of the Central Intelligence Agency. In October 1983, a suicide bomber detonated a truck full of explosives at a U.S. Marine Corps barracks located at Beirut International Airport. Casualties were 241 members of the U.S. Armed Services killed and more than 100 others wounded.[347]

In the United States, a domestic terrorist parked a truck bomb at the base of the Alfred P. Murrah Federal Building in April 1995, and casually detonated the truck bomb with a timed

---

[344] Steve Bowman, *Weapons of Mass Destruction: The Terrorist Threat*, 4.

[345] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, viii.

[346] "April 1983 US Embassy bombing," 1; available from http://encyclopedia.the freedictionary.com/April%2011983%20US%20Embassy%20bombing; Internet; accessed 1 July 2004.

[347] "Terrorist attacks on Americans 1979-1988," 2; available from http://www.pbs.org/wgbh/pages/frontline/shows/target/etc/cron.html; Internet; accessed 1 July 2004.

fuse. The high yield explosive was a relatively simple device using several thousand pounds of ammonium nitrate fertilizer, other materials, and explosives.[348] The blast and immediate aftermath killed 168 men, women, and children; and injured over 800 other people. The explosion devastated a large area of downtown Oklahoma City, Oklahoma.

Another horrific example of a high yield explosive and mass destruction is the near-simultaneous suicidal attack on the World Trade Center and Pentagon in September 2001. Other logical considerations for large volume explosive material include commercial shipping, railroad transportation, and major storage facilities.

Availability and Dual Use

The basic knowledge needed to produce an effective weapon of mass destruction can be found in college and medical school textbooks, advanced engineering books, magazines and periodicals, and on the Internet. With minimal training, individuals can produce various types of CBRNE weapons with relative ease in any home, school, or university laboratory, medical production or research facility, or commercial production facility. Minimal special equipment, purchased on the open market, can produce certain biological or chemical weapons. Weapons production cost is low, compared to other types of weaponry. Some precursor agents for biological and chemical production are dual use, are not expensive, and are not illegal to acquire or possess. Of course, theft, false documentation, and other techniques can surmount many of the normal regulatory control procedures for obtaining restricted precursor materials, equipment, or production processes.

Distinguishing legitimate biological, medical, or commercial production plants from a weapons production facility proves very difficult. Chemical and biological agents can be produced in small laboratories with little or no signature to identify the facility or their production. Normal biological warfare research facilities resemble completely legitimate bio-technical and medical research facilities. The same production facilities that can produce biological warfare agents may also produce wine and beer, dried milk, food and agricultural products.

Biological agents are naturally occurring and relatively easy to obtain as compared to nuclear material. They can be obtained from universities or medical schools. Chemical agents and their precursors can be obtained from civilian agriculture sites, textile, plastic, or civilian chemical production facilities, or military research and military facilities. Terrorist access to these weapons can also be through a state sponsor or, given the increasing sophistication of terrorist groups, might be manufactured in laboratories they have established and financed.

Security limitations for weapons of mass destruction in the former Soviet Union provide a possible resource for terrorists to acquire radiological or nuclear weapons. Additionally, radioactive materials or waste can be purchased legally and misused, or obtained illegally through black market transactions. Substances can be obtained from governmental or civilian research and medical facilities such as power plants, construction sites, laboratories, or

---

[348] Lou Michel and Dan Herbeck, *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing* (New York: Harper Collins Publishers Inc., 2001), 164.
.

hospitals, or from military facilities concerned with the storage, production, and weaponization of these materials.

A general concern exists that some unemployed scientists or weapons experts from the former Soviet Union are willing to sell their knowledge and services to other countries. However, the former Soviet Union is not the only potential source of concern. There are many other sources available, to include the United States. Chemical plants, biological labs, food irradiation plants, medical x-ray labs, and nuclear reactors and waste repositories are examples on a much larger list of possible sources for obtaining radiological material.

> **"When the spread of chemical and biological and nuclear weapons, along with ballistic missile technology – when that occurs, even weak states and small groups could attain catastrophic power to strike great nations. Our enemies have declared this very intention, and have been caught seeking these terrible weapons…"**
>
> **"The targets of these attacks are our military forces and our civilian population."**
>
> President Bush in The National Security Strategy of the United State of America

Conclusion

A complex contemporary environment becomes even more complex as governments, nation-states, and non-state organizations grapple with the issues on weapons of mass destruction counterproliferation and nonproliferation, and a growing access to technology and delivery means. Nations around the world have expanding nuclear energy programs, biological business conglomerates, and chemical industries that remain susceptible to terrorist penetration and attack. Weapons related technologies are ever more available in a world market, sometimes sanctioned by legitimate government regulation and sometimes beyond the constraint of rational controls. Rogue states demonstrate the willingness to supply specific WMD-related technology and expertise to other countries, or in extraordinary unilateral decisionmaking, to supply similar WMD expertise to non-state actors.[349]

---

[349] Director of Central Intelligence, DCI Weapons Intelligence, Nonproliferation, and Arms Control Center, *Unclassified Report to Congress on the Acquisition of Technology Reacting to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2003*, (Washington, D.C., January 2002), 11; available from http://www.cia.gov/cia/reports/721_reports/pdfs/jan_jun2003.pdf; Internet; accessed 19 May 2004.

> **"Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination."**
>
> President Bush in The National Security Strategy of the United State of America

In the foreseeable near future, the U.S. military remains an essential capability to demonstrate national awareness and commitment of our citizenry and elected civilian leaders, global leadership, enhanced intelligence and analyses, scientific and technological superiority, and resolve to protect the national security interests of the United States.[350] Several enabling functions stated in the U.S. *National Strategy to Combat Weapons of Mass Destruction* accent these priorities: intelligence collection and analysis on WMD, delivery systems, and related technologies; research and development to improve our ability to respond to evolving threats; bilateral and multilateral cooperation; and targeted strategies against hostile states and terrorists.

WMD is one of the most dangerous security issues that face the United States of America in the 21st Century. The three pillars of our *National Strategy to Combat Weapons of Mass Destruction* remains (1) counterproliferation, (2) nonproliferation, and (3) consequence management.[351] The U.S. military and civilian organizations understand the threat of WMD and remain ready to defend the Nations' people and resources. The United States must continue efforts – with friends, allies, and adversaries – to deter and dissuade the acquisition and use of weapons of mass destruction. When appropriate, preemptive action may be warranted to deny acquisition to WMD capabilities.

---

[350] Jon H. Moilanen, "Engagement and Disarmament: A U.S. National Security Strategy for Biological Weapons of Mass Destruction," *Essays on Strategy XIII*. (Washington, D.C.; National Defense University, 1996), 141-182.

[351] The White House, National Security Presidential Directive 17 (NSPD-17), *National Strategy to Combat Weapons of Mass Destruction*, (Washington, D.C., December 2002), 2; available from http://www.fas.org/irp/offdocs/nspd/nspd-17.html; Internet; accessed 8 December 2003.

Appendix H
WMD and CBRNE Consequence Management

The targets for terrorist WMD attacks are U.S. military forces and the civilian population.

U.S. National Security Strategy

General

"Defending the [U.S.] Nation against its enemies is the first and fundamental commitment of the U.S. Federal Government…The gravest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination…we must be prepared to defeat our enemies' plans, using the best intelligence and proceeding with determination."[352]

The U.S. National Security Strategy states a compelling requirement to stop rogue states and their terrorist clients before they are able to threaten or use weapons of mass destruction against the United States and our allies and friends.[353] National Security Presidential Directive 17, the *National Strategy to Combat Weapons of Mass Destruction*, calls for a comprehensive action plan to counter the threat of WMD in all of its dimensions. This strategy component is integral to the Global War on Terrorism (GWOT), U.S. homeland security, and other national strategies to defend and protect the United States. Three main pillars describe the essential aspects of combating weapons of mass destruction: counter proliferation, improved nonproliferation, and when necessary, effective consequence management to a WMD incident.

Figure. H-1. **Nuclear Plant Photo**
(*Source*: National Strategy for Homeland Security [minus reticle])

---

[352] The White House, *The National Security Strategy of the United Sates of America*, 1, 17 September 2002; available at http://www.whitehouse.gov/nsc/nss.html; Internet; accessed 30 April 2004.
[353] National Security Strategy, 9.

As a primary objective, terrorists attempt to create a demoralizing psychological effect on the target population and its leaders to erode resolve and enhance terrorist objectives. The characteristics of the United States – freedom, systems of movement, modern life, and prosperity – are all vulnerable to terrorism. Meanwhile, the distinction between domestic and foreign affairs is diminishing. The U.S. military and other appropriate agencies at Federal, state, and local levels of government must be prepared to deter and defend against the full range of possible WMD attack. Homeland security and transforming defense capabilities are part of this readiness. Of particular note, the U.S. must maintain the capability to reduce to the extent possible, the potentially horrific consequences of WMD attacks in the U.S. Homeland and at locations around the world.[354]
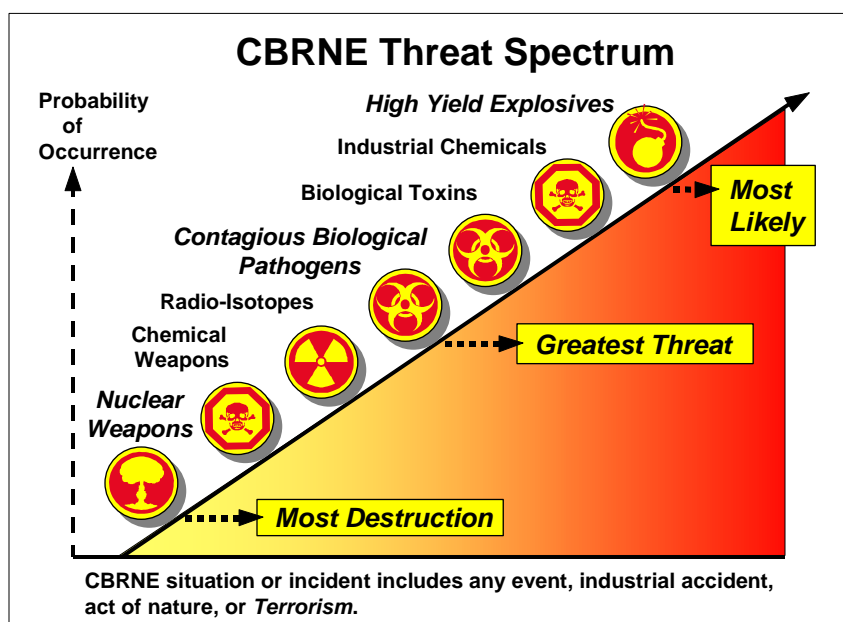

Figure H-2. CBRNE Threat Spectrum
(*Source*: JTF Civil Support Command Briefing 2004 and JHM).

To appreciate U.S. military capabilities for consequence management of a WMD incident, situational awareness must understand the probability of terrorist attack with chemical, biological, radiological, nuclear, or high yield explosive (CBRNE) attack. U.S. military capabilities are integral to a larger, robust national response to prevent or mitigate such attacks. The Department of Defense (DOD) supports this Federal mandate – the National Response Plan (NRP) – with centralized command and control and robust capabilities of DOD forces to assist a Lead Federal Agency (LFA) in a domestic WMD[355] incident by a CBRNE weapon, device, or material specifically designed to produce casualties or terror.

---

[354] The White House, National Security Presidential Directive 17 (NSPD-17), *National Strategy to Combat Weapons of Mass Destruction*, 2, December 2002; available at http://www.fas.org/irp/offdocs/nspd/nspd-17.html; Internet; accessed 8 December 2003.
[355] CJCSI 3125.01 *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Situation*, 3 August 2001.

One superb example of DOD consequence management capability is USNORTHCOM Joint Task Force Civil Support. However, to better appreciate the compelling requirements and capabilities of JTF Civil Support, the specter of WMD and terrorism must be fully understood.

Global Reach and WMD Terrorism

The probability of a terrorist organization using a chemical, biological, radiological, or nuclear weapon, or high yield explosive has increased significantly during the past decade.[356] The April 2004 attempt by terrorists to conduct near simultaneous bombings in Jordan with high yield explosives and chemical weapons spotlights the deliberate planning for use of weapons of mass destruction. Fortunately, Jordanian authorities foiled this attack on Jordanian and U.S. targets with a preemptive raid on terrorist facilities. Reports estimate that 20 tons of chemicals were confiscated and could have caused tens of thousands of casualties.[357] The intent of U.S. strategy is to stop terrorist attacks against the United States, its citizens, its interests, and its friends and allies around the world, and ultimately, to create an international environment inhospitable to terrorists and all those who support them.[358] The U.S. will not ignore regional or emerging threats, however, the operational efforts and intelligence will focus primarily on the most dangerous groups, namely, those terrorist groups with global reach or aspirations to acquire and use WMD.[359]

The 2004 U.S. National Military Strategy introduces an emergent term of weapons of mass destruction or effect (WMD/E). The term WMD/E relates to a broad range of adversary capabilities that pose potentially devastating impacts. WMD/E includes chemical, biological, radiological, nuclear, and enhanced high explosive weapons as well as other, more asymmetrical "weapons." They may rely more on disruptive impact than destructive kinetic effects. For example, cyber attacks on U.S. commercial information systems or attacks against transportation networks may have a greater economic or psychological effect than a relatively small release of a lethal agent.[360]

To enhance national security measures against terrorism and use of WMD, the U.S. uses several complementing strategies. Two of these strategies are the *National Strategy for Homeland Security* and the *National Strategy for Combating Terrorism*. Another directive is the *National Strategy to Combat Weapons of Mass Destruction*. While the strategy for homeland security focuses on preventing terrorist attacks within the United States, the strategy for combating terrorism focuses on identifying and defusing threats before they reach our borders.[361] Nonetheless, concepts of homeland security and combating terrorism, especially WMD and terrorism, are inseparable. U.S. strategic objectives seek to protect the U.S. from terrorism, reduce U.S. vulnerabilities, minimize damage, and recover from attacks that do occur.[362] In assessing functional capabilities, critical U.S. mission areas include:

---

[356] The White House, *National Strategy for Combating Terrorism*, 9, February 2003; available at http://www.state.gov/s/ct/rls/rm/2003/17798.htm; Internet; accessed 30 April 2004.
[357] "Jordan 'was chemical bomb target'," BBC News UK Edition, 17 April 2004; available at http://news.bbc.co.uk/1/hi/world/middle_east/3635381.stm; Internet; accessed 28 April 2004.
[358] National Strategy for Combating Terrorism, 11.
[359] Ibid., 16.
[360] Joint Chiefs of Staff, *National Military Strategy of the United States of America*, 1, May 2004.
[361] National Strategy for Combating Terrorism, 2.
[362] National Strategy for Homeland Security, vii.

intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response.[363]

Incidents of National Significance

Incidents that require Department of Homeland Security (DHS) operational and resource coordination are termed *Incidents of National Significance*, also referred to as nationally significant incidents or national incidents. Incidents requiring DHS action can include events such as: (1) credible threats, indications of terrorism or acts of terrorism within the United

Figure. H-3. WMD CBRNE Incident Management Phases
(*Source*: JTF Civil Support J5 2004 and JHM)
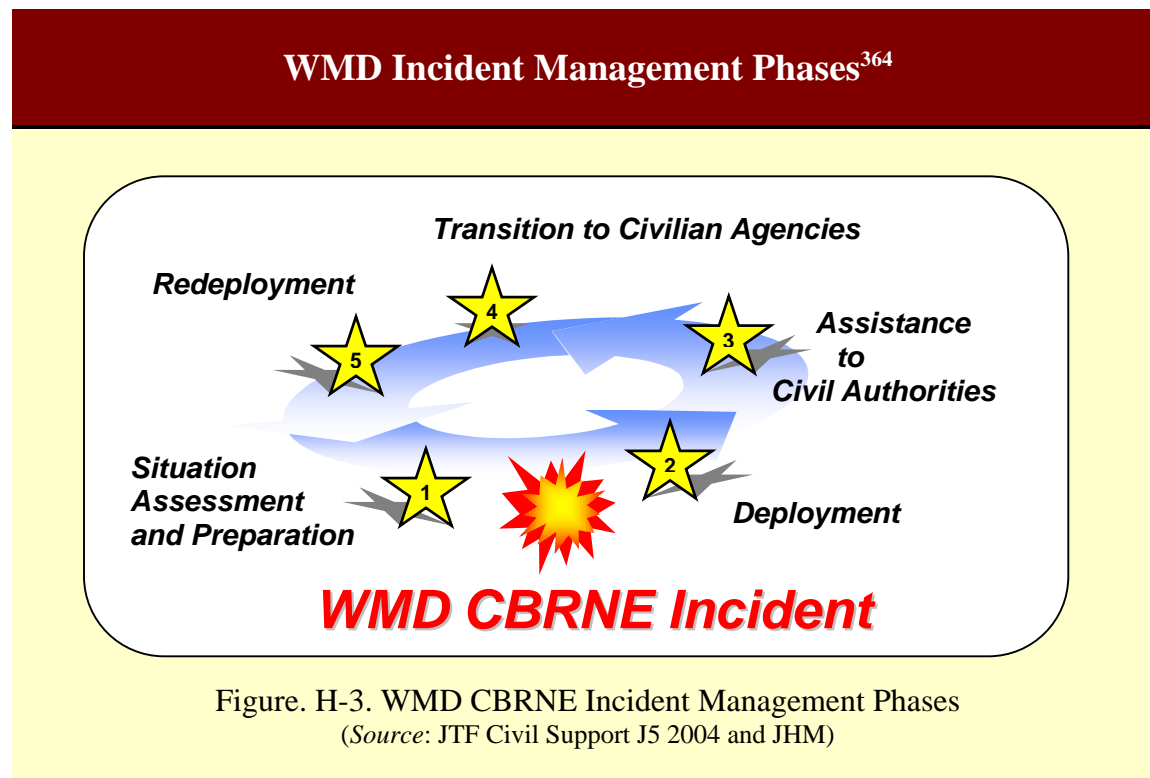
States; (2) major disasters or emergencies as defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act,[365] or any instances when the U.S. President determines that Federal assistance is needed to supplement state and local efforts to save lives and to protect property and public health and safety; (3) catastrophic natural or manmade incidents, including terrorism, that leave extraordinary levels of mass casualties, damage, and disruption severely affecting the population, infrastructure, environment, economy, and
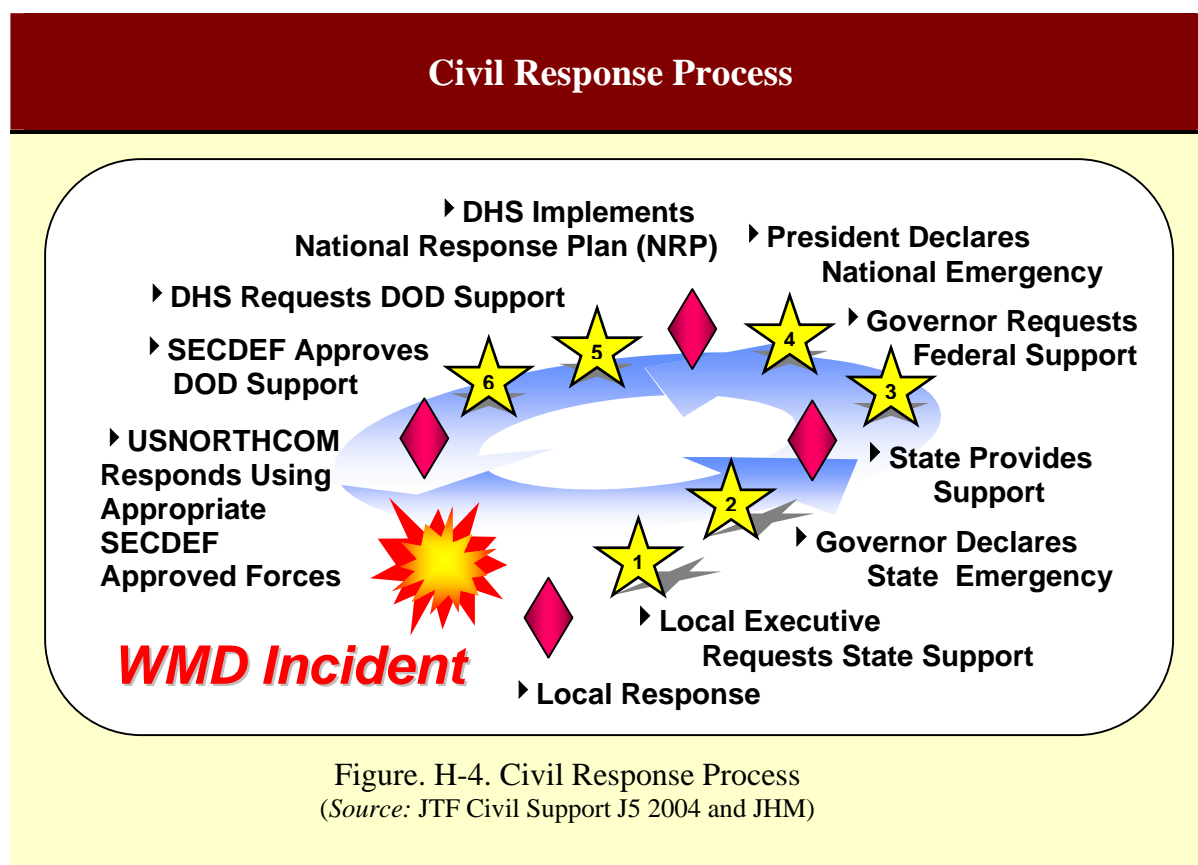
---

[363] Ibid., viii.

[364] See CJCS CONPLAN 0500-98, *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive Situation*, 11 February 2002.

[365] The *Robert. T. Stafford Disaster Relief and Emergency Assistance Act*, 42 U.S.C. 5121-5206, establishes the programs and processes for the Federal government to provide disaster and emergency assistance to States, local governments, tribal nations, individuals and qualified private non-profit organizations. The provisions of the Stafford Act cover all hazards including natural disasters and terrorist events. See glossary for an expanded description of significant provisions for DOD defense support to civilian authorities.

government functions; or (4) unique situations that may require coordination of incident management efforts.[366]

Crisis and the National Response Plan (NRP)

Response to national crises or consequence management to a catastrophic incident is shaping into a fully integrated national emergency response system. The Department of Homeland

Civil Response Process

▸ **DHS Implements National Response Plan (NRP)**

▸ **President Declares National Emergency**

▸ **DHS Requests DOD Support**

▸ **Governor Requests Federal Support**

▸ **SECDEF Approves DOD Support**

▸ **USNORTHCOM Responds Using Appropriate SECDEF Approved Forces**

▸ **State Provides Support**

▸ **Governor Declares State Emergency**

WMD Incident

▸ **Local Executive Requests State Support**

▸ **Local Response**

Figure. H-4. Civil Response Process
(*Source:* JTF Civil Support J5 2004 and JHM)

Security (DHS) is consolidating multiple Federal response plans into one all-discipline incident management plan. The Federal Response Plan (Final Draft) was published in June 2004. At the time of this writing, the NRP is emerging from final interim reviews with an expected publication date in 2004. The NRP serves as the core strategic national-level plan for coordinating Federal incident management activities for terrorist attacks or natural and manmade hazards, to save lives, protect public health, safety, property and the environment.[367]

The hazard-specific incident annexes in the NRP spotlight the type of national incidents, events, and hazards that may require a unified, specialized response: catastrophic incident; oil

---

[366] National Response Plan, Final Draft, 4 and 5, 30 June 2004; available at
https:www.niscc.org/downloads/NRP%20Final%20Draft%2030%20JUN%2004.pdf; Internet; accessed 4 October 2004.
[367] Ibid., 1 and 2

and hazardous substances; nuclear and radiological; biological; food safety and agriculture; cyber; and terrorism law enforcement and investigation. [368]

The Homeland Security Act of 2002 represents a crucial transition point in the way the Federal government organizes emergency response to WMD terrorism. The Act establishes the Department of Homeland Security (DHS), and consolidates the consequence management missions, assets, and personnel of numerous Federal departments and agencies into a single department. The primary missions of DHS include: preventing terrorist attacks within the United States; reducing the vulnerability of the United States to terrorism; and minimizing the damage and assisting in the recovery from terrorist attacks that occur within the United States.[369] The Homeland Security Act consolidates WMD consequence management assets and personnel under a single Federal agency, and serves as the legal impetus for a revised approach to WMD incident management.

HSPD-5 and the Federal Response Structure

Homeland Security presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, establishes a new approach to Federal emergency management of WMD events. The directive ensures that all levels of government across the nation have a single, unified, national approach toward managing domestic incidents. In conjunction with the *Homeland Security Act of 2002*, HSPD-5 tasks the Secretary of Homeland Security to develop and administer a National Response Plan that integrates Federal government domestic prevention, preparedness, response and recovery plans into one all-discipline, all-hazards plan. It also tasks the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS) that would unify Federal, state and local government capabilities within a National Response Plan framework to prepare for, respond to and recover from domestic events regardless of cause, size or complexity. These three echelons of government capability are three mutually supporting pillars of emergency response and civil support.

The intent behind the NRP and the NIMS is to provide the structure and mechanisms for establishing national level policy and operational direction regarding Federal support to state and local incident managers. Once finalized, the NRP will establish the Federal government's response policy, whereas the NIMS will serve as the operational arm of the NRP. The NIMS improves the chain of Federal command authority and coordination among the many Federal, state, and local organizations; improves planning and readiness; and integrates crisis and consequence management.

HSPD-5 also reaffirms the Secretary of Homeland Security's responsibility as the principal Federal official for domestic incident management. This coordination responsibility exists when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of state and local authorities are overwhelmed and Federal assistance has been requested by the appropriate state and local authorities; (3) more than one Federal department or agency

---

[368] Ibid., vi and vii
[369] Defense Threat Reduction Agency, *Domestic WMD Incident Management Legal Deskbook*, 3-12 and 3-13, December 2003; available at http://biotech.law.lsu.edu/blaw/DOD/manual; Internet; accessed 23 April 2004.

has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.

HSPD-5 also eliminates the previous division between crisis management[370] and consequence management[371] treating the two "as a single, integrated function, rather than as two separate functions." Whereas under the Federal Response Plan the Attorney General was the overall lead Federal official for the Government's response until the crisis management phase of the response was over, now the Secretary of Homeland Security remains the lead Federal official for the duration of the period involving Federal assistance. Despite HSPD-5 erasing the distinction between crisis management and consequence management, the directive reaffirms the Attorney General's authority as the lead official for conducting criminal investigation of terrorist acts or terrorist threats.[372]
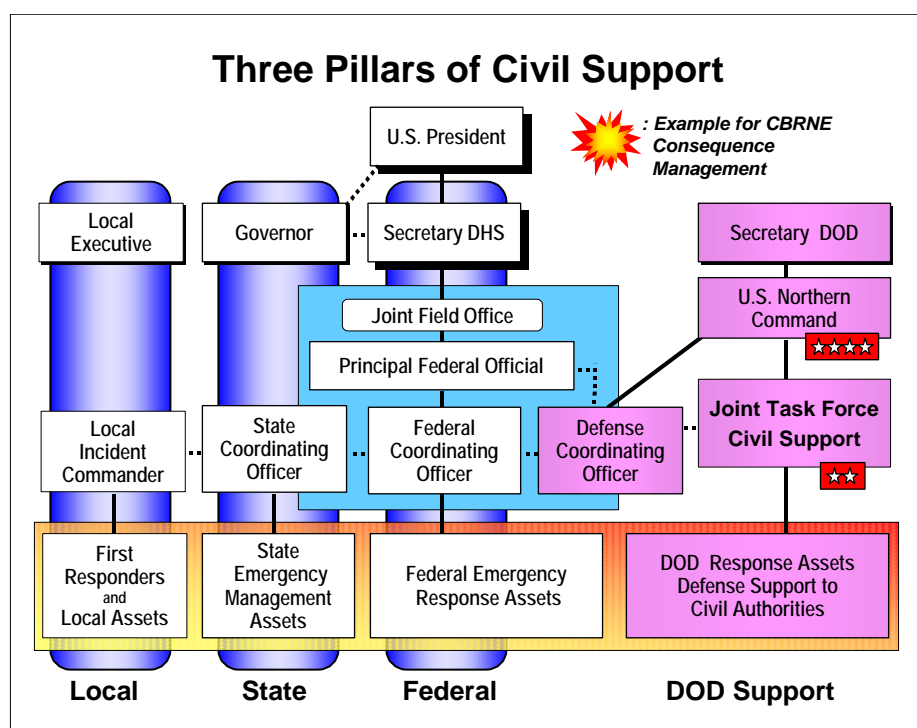

Figure. H-5. Three Pillars of Civil Support
(*Source*: JTF Civil Support Command Briefing 2004 and JHM)

---

[370] *Crisis Management*. Traditionally, crisis management was predominantly a law enforcement function and included measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The requirements of consequence management and crisis management are combined in the NRP.
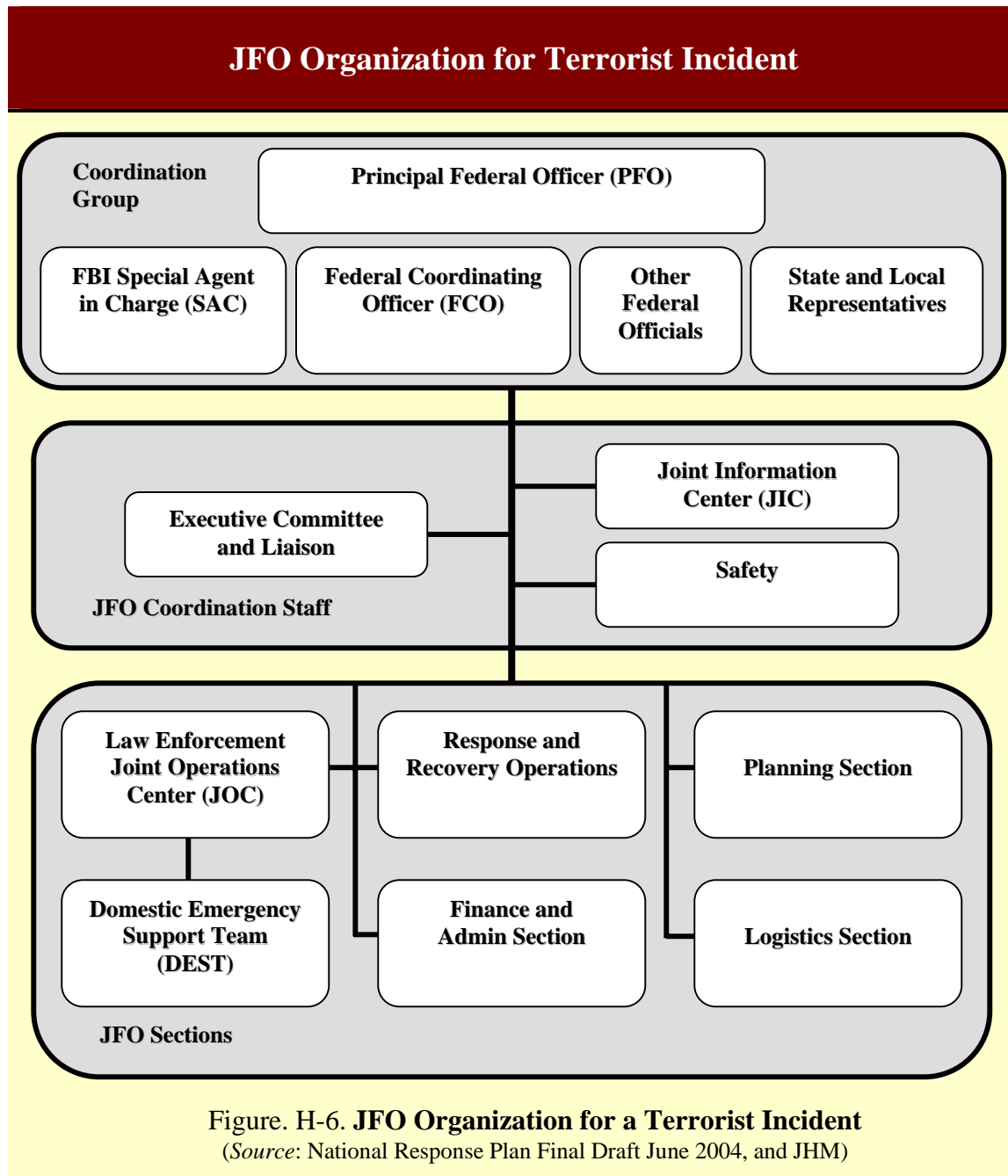
[371] *Consequence Management*. Traditionally, consequence management has been predominantly an emergency management function and included measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. The requirements of consequence management and crisis management are combined in the NRP.

[372] DTRA *Domestic WMD Incident Management Legal Deskbook*. 3-14.

Improvements to Incident Response

Approval of the Initial National Response Plan (INRP) and staffing of a final draft of the National Response Plan (NRP) provide improved incident management capability to the U.S. Several coordination processes and procedures implement a more effective emergency response. Some of the more visible capabilities are a National Homeland Security Operations Center (HSOC). The HSOC serves as the primary national-level hub for operational communications and information pertaining to domestic incident management. Located at

JFO Organization for Terrorist Incident

Coordination Group

Principal Federal Officer (PFO)

FBI Special Agent in Charge (SAC)

Federal Coordinating Officer (FCO)

Other Federal Officials

State and Local Representatives

JFO Coordination Staff

Executive Committee and Liaison

Joint Information Center (JIC)

Safety

JFO Sections

Law Enforcement Joint Operations Center (JOC)

Response and Recovery Operations

Planning Section

Domestic Emergency Support Team (DEST)

Finance and Admin Section

Logistics Section

Figure. H-6. **JFO Organization for a Terrorist Incident**
(*Source*: National Response Plan Final Draft June 2004, and JHM)

DHS headquarters, the HSOC provides full-time threat monitoring and situational awareness for domestic incident management. An Interagency Incident Management Group (IIMG), comprised of senior representatives from Federal departments and agencies, non-governmental organizations, as well as DHS components, facilitates national-level situation awareness, policy coordination, and incident coordination.

Correspondingly at an incident, Federal organization and principal leaders function, some with new titles and expanded responsibilities, for improved command and control, incident management and consequence management.

Joint Field Office (JFO). The JFO is a temporary Federal headquarters established to unify the Federal assistance effort with the state and local levels, and to coordinate the provision of Federal assistance to affected areas during national incidents. The JFO provides a central point for Federal, state, and local executives for incident oversight, direction, and assistance to effectively conduct and coordinate prevention, preparedness, response and recovery actions. The JFO leadership is responsible for coordination and integration of Federal operations and resources with state, local, private sector, and non-governmental organization incident command structures.

The JFO utilizes a scalable structure of the NIMS Incident Command System[373] and incident civilian "unified command."[374] The JFO organization adapts to the magnitude of the incident and supports NIMS principles regarding span of control and the five functions of: command, operations, planning, logistics, and finance/administration. Personnel from state and Federal departments and agencies provide staffing for the JFO generally through their respective Emergency Support Functions (ESF). The JFO replaces the Federal Emergency Management Agency (FEMA) Disaster Field Office (DFO) and manages all disaster assistance and other support. When activated for a terrorist incident, the JFO coordinates the functions of the Federal Bureau of Investigation (FBI) Joint Operations Center (JOC), and DHS/FEMA emergency preparedness and response and recovery actions within one Federal facility, when possible. Other Federal operations centers are encouraged to collocate with the JFO whenever possible.[375]

Emergency Response Team (ERT). The ERT is the principal interagency group that supports the PFO and FCO in coordinating the overall Federal incident operation. The ERT provides scalable staffing and organization for the JFO. Typically, the ERT encompasses the JFO Coordination Group, JFO Coordination Staff and the four JFO areas of operations, planning and information, logistics, and finance and administration. The ERT can be augmented by an advanced element known as the ERT-A. The ERT-A, in essence the nucleus of the eventual ERT, responds during the early stages of an incident to assess incident impact and identify specific state requests for Federal

---

[373] *The Incident Command System* (ICS) is a standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. The national standard for ICS is provided by NIMS.

[374] *Unified Command*, as a term in this Federal application of the Incident Command System (ICS), uses a definition of agencies working together through their designated Incident Commanders at a single Incident Command Post (ICP) to establish a common set of objectives and strategies, and a single Incident Action Plan. This is NOT "unified command" as defined by the Department of Defense.

[375] National Response Plan, Final Draft, 37 and 52.

incident management assistance. A national headquarters-level team known as the ERT-N can be deployed for large-scale high visibility events.

Principal Federal Official (PFO). The Secretary of DHS may designate a PFO to serve as the personal representative of DHS locally during an incident. The PFO oversees and coordinates Federal incident activities and works with local authorities to determine requirements and provide timely Federal assistance.

Principal Federal Official (PFO)

- **Represent Secretary of Homeland Security as lead Federal official on-scene.**

- **Ensure overall coordination of Federal domestic incident management activities and resource allocation on-scene.**

- **Ensure seamless integration of Federal incident management activities in support of state and local requirements.**

- **Provide strategic guidance to Federal entities.**

- **Facilitate interagency conflict resolution, as necessary.**

- **Serve as primary, although not exclusive, point of contact for Federal interface with state, local, and tribal government officials, media, and private sector.**

- **Provide real-time incident information, using the Federal incident management structure on-scene, to Secretary of Homeland Security through the Homeland Security Operations Center (HSOC) and Interagency Incident Management Group (IIMG), as required.**

- **Coordinate response resource needs between multiple incidents as necessary or as directed by the Secretary of Homeland Security.**

- **Coordinate overall Federal public communications strategy locally to ensure consistency of Federal interagency communications to the public.**

- **Ensure adequate connectivity is maintained between the JFO and HSOC; local, county, state, and regional EOCs; nongovernmental EOCs; and relevant elements of the private sector.**

- **Participate in on-going steady-state preparedness efforts, as pre-designated.**

Figure. H-7. **Principal Federal Official**
(*Source*: National Response Plan Final Draft June 2004, and JHM)

An "initial PFO" facilitates near-term Federal incident management activities until a longer-term PFO designate is assigned. The Secretary of DHS provides formal notification of the appointment of a PFO to the Governor of an affected state, and uses the HSOC to notify other Federal, state, local emergency operations centers.

Federal Coordinating Officer (FCO). The FCO manages Federal resource support activities related to Stafford Act disasters and emergencies. The FCO supports the PFO, when one is appointed, and is responsible for directing and coordinating the timely delivery of Federal disaster assistance resources. The FCO works closely with the PFO, Senior Federal Law Enforcement Official (SFLEO), and other Senior Federal Officials (SFOs) representing other Federal agencies engaged in the incident management.

Federal Coordinating Officer (FCO)

- **Conduct initial appraisal of the types of assistance most urgently needed.**

- **Coordinate timely delivery of Federal assistance to affected state and local governments, and disaster victims.**

- **Support the Principal Federal Officer (PFO), when designated.**

- **Serve as Disaster Recovery Manager (DRM) to administer the financial aspects of assistance authorized under the Stafford Act, when delegated.**

- **Work in partnership with the State Coordinating Officer (SCO) appointed by the Governor to oversee operations for the state, and the Governor's Authorized Representative (GAR) empowered by the Governor to execute all necessary documents for Federal assistance on behalf of the state.**

- **Take other such actions consistent within the delegated authority deemed necessary to assist local citizens and public officials in promptly obtaining assistance to which they are entitled.**

Figure H-8. **Federal Coordinating Officer**
(*Source*: National Response Plan Final Draft June 2004 and JHM)

The FCO may also be designated to coordinate resources in non-Stafford Act situations. In order to provide Federal-to-Federal support in these instances, the FCO utilizes the authority issued to DHS under HSPD-5. In these situations, the FCO requests support from other Federal departments and agencies using interagency agreements and memoranda of understanding rather than the mission assignment process used for Stafford Act disasters and emergencies. [376]

---

[376] National Response Plan [DHS], Draft #1, 19 and 20, 25 February 2004; and Final Draft, 44; June 2004.

Domestic Emergency Support Team (DEST). The DEST is a rapidly deployable, specialized interagency team designed to provide expert advice, guidance and support to the FBI Senior Agent in Charge (SAC) and PFO during a WMD incident or credible threat. [377]

For terrorist incidents, the President's responsibilities for coordinating and conducting law enforcement and criminal investigation activities are executed by the Attorney General acting through the FBI. During the terrorist incident, the local FBI Senior Agent in charge (SAC) coordinates these activities with the other members of the law enforcement community, and works in conjunction with the PFO who coordinates overall Federal incident management activities at the local level.[378]

Homeland Security and DOD Military Forces

The Department of Defense (DOD) primarily maintains readiness to defend the USA. DOD also maintains readiness to provide military support to civilian authorities (MSCA) when directed to do so by the U.S. President. The role of DOD in homeland security continues to gain definition. Currently, homeland security is a concerted national effort to prevent terrorist attacks within the U.S., reduce U.S. vulnerability to terrorism, minimize damage, and assist in the recovery from attacks.

The DOD role in homeland security is: (1) homeland defense as the military protection of United Sates territory, domestic population, and critical defense infrastructure and assets from external threats and aggression; and (2) civil support as the support to U.S. civil authorities for domestic emergencies and for designated law enforcement and other activities.[379] U.S. Northern Command (USNORTHCOM) was created to improve command and control of DOD forces in homeland defense and civil support missions.

For homeland defense, the DOD Services (Army, Navy, Marines, Air Force) provide USNORTHCOM, and in specific cases U.S. Pacific Command (USPACOM), with capabilities that span air, land, and sea areas as well as selected critical infrastructure. USNORTHCOM's area of responsibility comprises the air, land, and sea approaches from 500 nautical miles to the United States coastline, the continental United States itself, Alaska, Canada, Mexico, Puerto Rico, and the Virgin Islands. Hawaii and the U.S. territories and possessions in the Pacific remain the responsibility of the Pacific Command. For increased domestic airway security, USNORTHCOM coordinates the capabilities of North American Aerospace Defense Command (NORAD) and the Federal Aviation Administration. Federalized National Guard units are another capability that USNORTHCOM coordinates for homeland security efforts.[380] Numerous other DOD support capabilities exist. [381]

---

[377] National Response Plan, Final Draft, 52, June 2004.
[378] Ibid., 22.
[379] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, (Washington, D.C., September 2003), 1.
[380] Steve Bowman, *Homeland Security: The Department of Defense's Role*, Congressional Research Service Report for Congress, Order Code RL 31615, 7, 14 May 2003.
[381] Congressional Research Service, Homeland Security: The Department of Defense's Role RL 31615, 7.

The National Guard has Weapons of Mass Destruction Civil Support Teams (WMD-CST) that are full-time active duty personnel whose mission is to assess a suspected CBRN[382] incident, advise civilian authorities, and expedite the arrival of additional military personnel. They can be employed in a Federal or a non-Federal status. The National Guard is normally employed in a non-Federal status, under state control, to meet the needs of state and local authorities. Each team consists of 22 personnel and is equipped with CBRN detection, analysis, and protective equipment. The U.S. Congress has authorized 55 WMD-CSTs to ensure that each state and territory has a team. Over half of the 55 authorized teams are certified with requisite training and equipment. Remaining teams are still being staffed and equipped.[383] Additionally, the U.S. Marine Corps maintains a Chemical, Biological Incident Response Force that is capable of consequence management.

The U.S. Navy has been tasked to support USNORTHCOM's mission to deter and defend against hostile action from maritime threats by providing defense in depth that is seamless, unpredictable to our enemies, and able to defeat threats at a maximum distance from U.S. territory. The Navy maintains alert ships and aircraft on both coasts and the Gulf of Mexico for this mission. [384]

The U.S. Air Force has increased its "24 hours a day, 7 days a week" capabilities in a variety of ways to respond to Federal taskings under Title 10 and non-Federal taskings and Title 32 (Federally funded, state controlled) authorities. Extensive mobilization of Guardsmen and Reservists provide a robust capability posture. Aircraft Alert Posture sites have more than doubled since September 11, 2001. Combat air patrols are employed for national security special events (NSSEs) and other designated public venues, as required. The Air Force Auxiliary (Civil Air Patrol) provides additional capacity to support USNORTHCOM, other Federal agencies, and state and local governments. [385]

DOD and Defense Support to Civil Authorities

The Department of Defense provides Defense Support of Civil Authorities (DSCA) [a new term in the draft National Response Plan] in response to requests for Federal assistance during domestic terrorist attacks, major disasters, and other emergencies. Although current DOD Directives use terms of Military Assistance to Civil Authorities (MACA) and Military Support to Civil Authorities (MSCA), DOD is considering DSCA as an overarching civil support term. Future DOD Directives may use DSCA to coincide with the final National Response Plan. DSCA refers to DOD support of civil authorities for domestic emergencies, and for designated law enforcement and other activities. This support includes DOD civilians and DOD contractors, and Federal military forces.[386]

---

[382] *CBRN*: Chemical, biological, radiological, and nuclear weapons.

[383] Congressional Research Service, *Homeland Security: The Department of Defense's Role* RL 31615, 9; and, Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security,* 8.

[384] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, (Washington, D.C., September 2003), 6.

[385] Ibid., 7.

[386] National Response Plan [DHS], Draft #1, 37; and Final Draft, 53.

Defense support is a very complex functional entity and requires broad cooperation with Federal, state, and local elements. DOD will normally provide support only when other local, state or Federal resources are unavailable and only if Defense support does not interfere with DOD's primary mission or ability to respond to operational contingencies.

The primary focus of intelligence collection and analysis within the DOD is on the foreign threat and on the generation of intelligence for the protection of U.S. forces at home and abroad. Terrorism that targets the homeland is fundamentally a law enforcement requirement best addressed by domestic law enforcement organizations. DOD may have a supporting role during crises. DOD has a responsibility to protect its forces, capabilities, and infrastructure within the United States. Along with Service and DOD law enforcement/counterintelligence organizations and USNORTHCOM, many Federal, state, and local organizations outside DOD have significant roles in collecting and analyzing information and intelligence, and in conducting investigations and operations to prevent or preempt terrorist attacks.

The traditional military assistance to civilian authorities (MACA)[387] encompasses military support to civil authorities (MSCA),[388] military assistance for civil disturbances (MACDIS),[389] and military assistance to law enforcement (MACLEA). Assistance and support include capabilities for immediate response, loan of materiel, and people with subject matter expertise in functional emergency support. Military support to civilian authorities may also take the form of providing technical support and assistance to law enforcement, assisting in the restoration of law and order, providing specialized equipment, and assisting in consequence management.[390]

Two circumstances exist for DOD providing Defense Support to Civil Authorities:

- In emergency circumstances, such as managing the consequences of a terrorist attack, major disaster, or other emergency, DOD could be asked to act quickly to provide capabilities that other agencies do not possess or that have been exhausted or overwhelmed.

- In non-emergency circumstances of limited scope or planned duration, DOD would support civil authorities where other Federal agencies have the lead – for example, providing security at a special event such as the Olympics, or assisting other Federal agencies to develop capabilities to detect chemical, biological, nuclear, and radiological threats.

Civil support missions are supported by DOD when involvement is appropriate and when a clear end state for DOD participation is defined. DOD will seek reimbursement for civil support missions when authorized by U.S. law. Representative examples of DOD support of civil authorities are: DOD support to the Federal Bureau of Investigation (FBI) for crisis management, law enforcement, intelligence support, and domestic counter terrorism activities; DOD support to the U.S. Coast Guard, including surveillance, patrol, and escort in the maritime domain and specialized support, such as Explosive Ordnance Disposal (EOD),

---

[387] DOD Directive 3025.15, Military Assistance to Civil Authorities, 18 February 1997.
[388] DOD Directive 3025.1, Military Support to Civil Authorities (MSCA), 15 January 1993.
[389] DOD Directive 3025.12, Military Assistance for Civil Disturbances (MACDIS), 4 February 1994.
[390] National Strategy for Homeland Security, 44.

Mine Countermeasures (MCM), and intelligence; or DOD support to the Department of Homeland Security (DHS), including support for domestic consequence management in the event of a chemical, biological, radiological, nuclear, or high-yield explosive terrorist attack.

Under the provisions of the Stafford Act, DOD support for disaster relief must be requested. (The other principal statute under which DOD provides emergency support is the Economy Act, under which any Federal agency can request support on a reimbursable basis from DOD.) Prior to appointment of a DCO, requests for Defense support are made through the Department of Defense Executive Secretary within the Office of the Secretary of Defense.

Defense Coordinating Officer (DCO)

Following appointment of a DCO, all requests for Defense support at the incident site management location are processed through the DCO. A Defense Coordinating Element (DCE) provides logistical and administrative support to the DCO. The DCO serves as *the single point of contact* at an incident site for coordinating and validating the use of DOD resources. The DCO will collocate with the PFO and FCO in the Joint Field Office.

Defense Coordinating Officer (DCO)

- **Act as the designated DOD on-scene representative at JFO.**

- **Act as the single point of contact (POC) at the incident management location for coordinating and validating the use of DOD resources.**

- **Coordinate Request for Assistance (RFA) and mission assignments with the FCO or designated Federal representative.**

- **Operate as DCO/DCE within the Joint Field Office (JFO).**

- **Direct on-scene support of Defense Coordinating Element (DCE), comprising administrative staff and liaison personnel, including Emergency Preparedness Liaison Officers (EPLO).**

- **Forward mission assignments to appropriate military organizations through DOD-designated channels.**

Figure. H-9. **Defense Coordinating Officer**
(*Source*: National Response Plan Draft/Final Draft June 2004 and JHM)

Upon execution of the NRP, requests for Defense support must be accompanied by a Request for Federal Assistance (RFA) form, unless the DOD component is responding under its independent funding authority or the commander's immediate response authority as defined in

DOD Directive 3025.1. Some exceptions exist in requesting Defense Support to Civil Authorities such as Army Corps of Engineers (ACE) support, National Guard forces operating in State Active Duty or U.S. Title 32 status, or DOD forces in support of the FBI.[391] An authorizing official of the requesting agency validates and submits a Requests For Assistance (RFA) along with a fund cite.

Once the DCO validates the request, the DCE forwards the request directly to the supported combatant commander, or to the supporting headquarters designated by the combatant commander for execution. At times DOD provides, through the combatant commander, a joint task force (JTF) for command and control of DOD military forces.[392] In this case, the DCO will normally work for the JTF commander as a special staff officer and closely coordinate with the task force operations section. The DCO remains the focal point in the joint field office for requests for military support from the PFO or FCO, and after validation by the FPC or FCO, passes the requests to the JTF staff or other DOD organizations.

DOD has a variety of relationships with state and local governments independent of those between state National Guard forces and DOD. The Army, Navy, Air Force, and Marine Corps Reserve provide Emergency Preparedness Liaison Officers (EPLO) to state and regional emergency response operations. The Emergency Preparedness Liaison Officer (EPLO) Program establishes liaison officers and support personnel in each state, with duty at the Governor's respective Department of Military Affairs or State Department of Defense, under the States' Adjutant Generals to coordinate mutual DOD support for national security emergency preparedness, response to natural or man-made disasters, and other domestic emergencies.[394]

On a case-by-case basis, people, units, equipment, and other DOD resources can be ordered to support a civil emergency; however, reservists cannot be ordered involuntarily to active duty solely to respond to a civil emergency except for extraordinary authorized circumstances in response to a CBRNE event.[395]

Army and Air National Guard forces, acting under state authority of the Governor (that is, not in Federal service), have primary responsibility for providing military assistance to state and local government agencies in civil emergencies within their respective states. The Guard includes highly specialized capabilities such as those provided by the state-controlled Weapons of Mass Destruction Civil Support Teams (WMD-CST). When such units, or other

---

[391] National Response Plan Final Draft, 54.

[392] Army War College, *How The Army Runs; A Senior Leader Reference Handbook 2003-2004*, U.S. Army War College, (Carlisle, PA: Department of Command, Leadership, and Management, 23 September 2003), 472; available at http://carlisle-www.army.mil/usawc/dclm/linkedtextchapters.htm; Internet; accessed 31 December 2003.

[393] Army War College, *How The Army Runs; A Senior Leader Reference Handbook 2003-2004*, U.S. Army War College, (Carlisle, PA: Department of Command, Leadership, and Management, 23 September 2003), 472; available at http://carlisle-www.army.mil/usawc/dclm/linkedtextchapters.htm; Internet; accessed 31 December 2003.

[394] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 15.

[395] Army War College, *How The Army Runs; A Senior Leader Reference Handbook 2003-2004*, U.S. Army War College, (Carlisle, PA: Department of Command, Leadership, and Management, 23 September 2003), 481; available at http://carlisle-www.army.mil/usawc/dclm/linkedtextchapters.htm; Internet; accessed 31 December 2003.

National Guard units and personnel, are directed to Federal service (Title 10 duty), they will respond to requirements validated by the designated DOD Defense Coordinating Officer.

Each DOD active and reserve installation maintains a relationship with local authorities from surrounding jurisdictions by virtue of proximity and their authority to provide immediate response. As DOD policy, a DOD installation commander may take immediate action to assist civil authorities or the public to save lives, prevent human suffering, or mitigate significant property damage under many imminently serious conditions that occur where there has been insufficient time to obtain approval through the chain of command and there has not been any declaration of major disaster or emergency by the U.S. President.

Installation commanders support area community relations with the local governments in order to address local security issues. DOD often participates in state-sponsored councils that focus on specific homeland security issues. USNORTHCOM works with both the regional and state-level Emergency Preparedness Offices to coordinate capabilities, plans, and operations. USNORTHCOM also includes state and regional level emergency response organizations in training activities and homeland defense exercises.[396]

Responsibilities of the DCO can be modified based on specific situations; however, normal functions include validating requests for Defense support and forwarding mission assignments to an appropriate military organization; and assigning military liaison officers to provide technical assistance to applicable activated Emergency Support Functions (ESF). The DCO, through appropriate military channels, refers contentious Defense support issues to the Assistant Secretary of Defense for Homeland Defense.[397]

DOD Authority

The Secretary of Defense maintains authority over DOD and conducts his responsibility in the chain of command for employing DOD forces under a military command and control system. The Secretary of Defense provides authorized and appropriate Defense support to civil authorities for domestic incidents, as directed by the President, or when consistent with military readiness and appropriate under the circumstances and the law. The chain of command for military forces providing Defense support of civil authorities remains constant and unchanged. Command for military forces is a direct link from the President, to the Secretary of Defense, to the Commander of a combatant command and to a joint task force. For example, USNORTHCOM has command over the commander of Joint Task Force Civil Support.

Accordingly, the civilian "unified command" concept used widely by civil public safety authorities as part of the emergency response and the Incident Command System (ICS), does _not_ include DOD forces.[398]

---

[396] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 15.
[397] National Response Plan, Final Draft, 54.
[398] Ibid., 14.

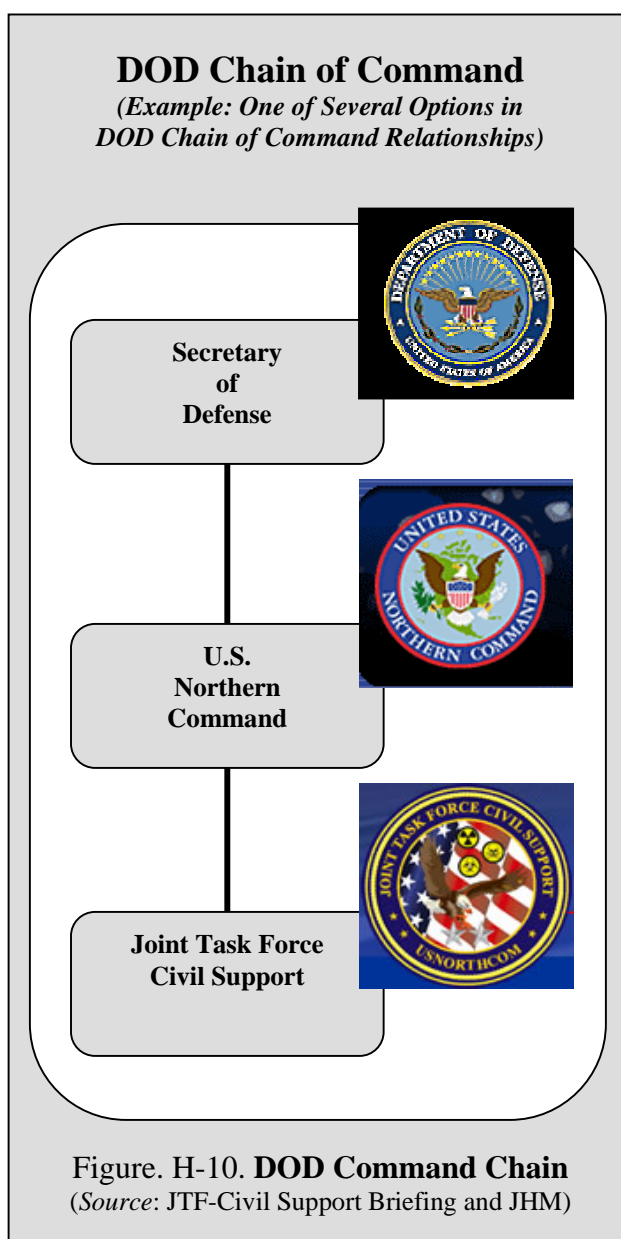**U.S. Northern Command (USNORTHCOM)**

A 2002 revision of the U.S. Unified Command Plan (UCP) established a new combatant command, U.S. Northern Command. USNORTHCOM is responsible for homeland defense and for assisting civil authorities in accordance with U.S. law. The commander of USNORTHCOM receives all operational orders from the U.S. President, through the Secretary of Defense.[399]

The Army maintains forces on a graduated response posture ready to support homeland defense missions. The Army also identifies multiple units ready to provide consequence management augmentation for Joint Task Force Civil Support, if required and directed by the Secretary of Defense. The Army continues to identify units ready to support the DOD Civil Disturbance Plan should that be required and directed by the Secretary of Defense.[400] The Army, in collaboration with the Air Force, is also developing enhanced capabilities to protect sites within the homeland from air attack. Additionally, the U.S. Navy works in conjunction with the U.S. Coast Guard to provide protection from maritime attacks.

U.S. Northern Command takes the homeland defense missions being performed by other Department of Defense organizations and places them within a single combatant command. Simultaneously, U.S. Northern Command plans, organizes, and executes civil support missions.

The USNORTHCOM mission is homeland defense and civil support. Specifically, this combatant command:

- Conducts operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility.

DOD Chain of Command
(Example: One of Several Options in DOD Chain of Command Relationships)

Secretary of Defense

U.S. Northern Command

Joint Task Force Civil Support

Figure. H-10. **DOD Command Chain**
(*Source*: JTF-Civil Support Briefing and JHM)

---

[399] National Strategy for Homeland Security, 44 and 45.
[400] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 5.

- As directed by the President or Secretary of Defense, provides military assistance to civil authorities including consequence management operations.

Reserve Components

The relationship between the DOD, including its combatant commands, and the National Guard and Reserve is the same with respect to homeland security roles as it is in a warfighting context. In cases where the governors of the states and territories employ National Guard forces in a state status to perform state missions of a homeland security nature, those National Guard forces have no direct operational relationship to the Department or its combatant commands. However, the National Guard and Reserve components represent the nation's strategic reserve of organized military capability, and are critical to DOD ability to sustain long-term military operations.

National Guard personnel serving in a State Active Duty or Title 32 status remain subject to recall to active duty under Title 10 to meet Federal requirements. The Chairman, Joint Chiefs of Staff, maintains visibility of National Guard assets performing homeland security missions, as do combatant commanders in order to adjust warfighting plans if necessary to overcome reductions in assigned capabilities. Moreover, USNORTHCOM and PACOM must have visibility of state controlled National Guard operations to facilitate coordination between Title 10 and Title 32 or State Active Duty military operations, which might be occurring in the same area, at the same time, towards a common objective.[401]

Federal Military Forces and U.S. Law

The USNORTHCOM homeland defense mission is directed against military threats emanating from outside the United States. USNORTHCOM has a cooperative relationship with Federal agencies working to prevent terrorism. These organizations share information and work together to coordinate plans and actions. This level of cooperation and information sharing improves the effectiveness of homeland security efforts overall and enhances prevention of threats, attacks and other acts of aggression against the United States. Notwithstanding, many organizations at local, state and Federal levels have important roles in collecting intelligence, investigating, and then conducting the operations to preempt terrorism. The *Posse Comitatus Act*[402] prevents the Federal U.S. military from direct law enforcement involvement.

A significant difference between homeland security and homeland defense is the limitations on use of Federal military forces. USNORTHCOM is a military organization whose operations within the United States are governed by Federal law that prohibits direct military involvement in law enforcement activities. DOD and USNORTHCOM roles in support of homeland security are limited to homeland defense and civil support.

---

[401] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 15 and 16.

[402] The *Posse Comitatus Act*, 18 U.S.C. 1385, prohibits the use of the Army or the Air Force for law enforcement purposes, except as otherwise authorized by the Constitution or statute. This prohibition applies to Navy and Marine Corps personnel as a matter of DOD policy. The primary prohibition of the *Posse Comitatus Act* is against direct involvement by active duty military personnel (to include Reservists on active duty and National Guard personnel in Federal service) in traditional law enforcement activities (to include interdiction of vehicle, vessel, aircraft, or other similar activity; a search or seizure; an arrest, apprehension, stop and frisk, or similar activity).

Terrorism targeted against the United States is fundamentally a homeland security matter usually addressed by law enforcement agencies. Homeland security is the prevention, preemption, and deterrence of, and defense against, aggression targeted at U.S. territory, sovereignty, domestic population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies. Homeland security is a national team effort that begins with local, state and Federal organizations. Homeland defense (HLD) is the protection of U.S. territory, domestic population and critical infrastructure against military attacks emanating from outside the United States.

Defending Against WMD Threats - CBRNE

The United States of America is the world's fourth largest nation with 3.5 million square miles of land and 88,000 miles of tidal shoreline. Each year, 11.2 million trucks and 2.2 million rail cars cross into the U.S. from the 7,500-mile land and air border shared with Canada and Mexico. Over 7,500 foreign-flag ships make 51,000 calls annually to U.S. ports. The country routinely admits millions of visitors from around the world.[403]

Underlying these social, economic, and political arenas, ruthless and resourceful terrorists seek to threaten the U.S. with new technologies, dangerous weapons, and nontraditional tactics that exploit our freedoms. As the nation witnessed on September 11, 2001, enemies of the U.S. have the resolve and means to commit acts of terrorism and mass destruction against innocent civilians and commercial interests within our country.

Having few permanently assigned forces, USNORTHCOM will be assigned forces whenever necessary to execute missions as ordered by the President and as provided by the U.S. Armed Services.   Yet, several pre-existing joint force headquarters have been assigned to USNORTHCOM with the ability to execute missions such as counterdrug assistance, homeland security, homeland defense, and civil support for CBRNE consequence management on a daily basis.

An Army core competency is to support civil authorities.[404] With the establishment of USNORTHCOM, the Commander of U.S. Forces Command (USFORSCOM) serves in the role of the Army Service Component Commander for USNORTHCOM. Headquarters, USFORSCOM retains its role as a force provider and remains assigned to U.S. Joint Forces Command (JFCOM).[405]

USFORSCOM is U.S. Northern Command's coordinating authority for military support to civil authorities (MSCA) and supports domestic emergencies through its two Continental U.S. Army (CONUSA) headquarters. Both First Army and Fifth Army have assigned areas of responsibility that approximate the eastern and western half of the USA with specified

---

[403] NORTHCOM [U.S. Northern Command] website; available at http://www.northcom.mil; Internet; accessed 28 April 2004.

[404] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 5.

[405] Ibid., 6

additions. U.S. Pacific Command (USPACOM) provides MACA within its extensive assigned area of responsibility.[406]

The Armed Services provide increased homeland security and disaster response capabilities to the U.S. in support of the charter of the Department of Homeland Security. Ground, air, space, and maritime areas of interest align Army, Navy, Air Force, and Marine Corps capabilities to support governmental programs such as air defense, inland waterways, port facilities, and border and critical infrastructure security. One example of a specific disaster response asset is the Marine Corps' Chemical, Biological Incident Response Force (CBIRF) and other Marine Corps assets. Tasks include detecting terrorist actions, deterring terrorist acts, defending specified locations, and conducting initial incident response to chemical, biological, radiological, or nuclear terrorist attacks.[407]

The specter for weapons of mass destruction is a range of capabilities spanning chemical, biological, radiological, nuclear, and high yield explosives (CBRNE). Incidents that may cause catastrophic damage and destruction include industrial accidents, acts of nature, acts of war, and terrorism. Effective CBRNE response requires a distinct and deliberate set of resources, skills and experience.

Understanding Joint Task Force Civil Support (JTF-Civil Support)

The purpose of Joint Task Force Civil Support is to save lives, prevent injury and provide temporary critical life support during a chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) situation in the United States or its territories and possessions. JTF-Civil Support is the only U.S. military organization dedicated solely to planning and integrating Department of Defense forces for consequence management (CM) support to civil authorities.

As a standing joint force headquarters, JTF-Civil Support comprises active component, reserve component and National Guard members from the Army, Navy, Air Force, Marines and Coast Guard, as well as civilian personnel, and is commanded by a federalized Army National Guard General Officer. The joint task force stands ready to aid the designated Lead Federal Agency (LFA), most likely the Federal Emergency Management Agency (FEMA), in charge of managing the consequences of a CBRNE accident or incident. A former independent agency tasked with planning for and responding to disasters, FEMA is now a part of the Department of Homeland Security.

When directed by the Commander of U.S. Northern Command, JTF-Civil Support will deploy to the incident site, establish command and control of designated DOD forces, and provide military assistance to civil authorities to save lives, prevent injury and provide temporary critical life support in order to reduce the harmful effects of a CBRNE incident.

---

[406] Army War College, *How The Army Runs: A Senior Leader Reference Handbook 2003-2004*, 474.
[407] Department of Defense, *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security*, 5 to 8.

Within its USNORTHCOM Charter, JTF-Civil Support is a standing Joint Task Force headquarters under the combatant command (COCOM)[408] of Commander, USNORTHCOM, and is authorized several command relationships. USNORTHCOM is the Supported Combatant Commander within its area of responsibility (AOR) and will normally maintain both administrative control (ADCON)[409] and operational control (OPCON)[410] of JTF-Civil Support. During domestic situations in the USPACOM AOR, USNORTHCOM will be a Supporting Combatant Commander and, when directed by the SECDEF, will transfer OPCON of JTF-Civil Support to the Supported Combatant Commander.

Subordinate units or elements of JTF-Civil Support will normally be either attached,[411] OPCON, or TACON[412] for command or control to the Commander of JTF-Civil Support by USNORTHCOM to accomplish mission tasks.

The Commander of JTF-Civil Support, when directed, will exercise OPCON over the Defense Coordinating Officer (DCO) and the Defense Coordinating Element (DCE) during a CBRNE situation. Located in the Joint Field Office, the DCO works closely with the Federal Coordinating Officer (FCO) or other senior DHS (FEMA) officials on the scene.

When coordinated by USNORTHCOM, the Commander JTF-Civil Support is granted Direct Liaison Authorized (DIRLAUTH) with designated Initial Entry Force (IEF) units for CBRNE CM information sharing, exercise and operational planning, and interoperability issues. DIRLAUTH and coordination does not include tasking authority unless OPCON or TACON of tasked forces is specifically authorized. DIRLAUTH is authorized with other DOD

---

[408] Combatant Command (Command Authority) (COCOM). (DOD) Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) can<u>not</u> be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Operational control is inherent in combatant command (command authority). (JP 1-02); available at http://www.au.af.mil/au/awc/awcgate/pub1/appendix_g.pdf; Internet; accessed 26 May 2004.

[409] Administrative Control (ADCON). (DOD) Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. (JP 1-02)

[410] Operational Control (OPCON). (DOD) Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. (JP 1-02)

[411] Attach. (DOD) 1. The placement of units or personnel in an organization where such placement is relatively temporary. 2. The detailing of individuals to specific functions where such functions are secondary or relatively temporary, e.g., attached for quarters and rations; attached for flying duty. (JP 1-02)

[412] Tactical Control (TACON). Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and, usually, local direction and control of movements or maneuvers necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. See also combatant command; combatant command (command authority); operational control. (JP 1-02)

CBRNE CM capable units and Defense agencies to enhance operational planning.[413]   Again, DIRLAUTH and coordination does not include tasking authority unless OPCON or TACON of the tasked forces is specifically authorized.

Through the National Guard Bureau, the Commander JTF-Civil Support is granted DIRLAUTH with each state-level National Guard Joint Force Headquarters, to include National Guard Weapons of Mass Destruction-Civil Support Teams (WMD-CSTs), for coordination and planning that supports the overall military capabilities for CBRNE emergency response.   The Commander JTF-Civil Support informs and updates USNORTHCOM, Service Component Headquarters, the Chief of the National Guard Bureau, and The state Adjutants General (TAGs) of ongoing coordination, planning, and actions.

The primary mission authority allowing DOD to engage in domestic consequence management operations is the Robert T. Stafford Disaster Relief and Emergency Assistance Act. The Stafford Act authorizes the President to provide disaster and emergency assistance to state and local governments upon receipt of a request from a Governor. Deployment of JTF- Civil Support, at the direction of the Commander of U.S. Northern Command, and on the authority of the Secretary of Defense, would occur only after a Governor requests Federal assistance from the President, and after the President issues a Presidential Disaster Declaration.

Preparing for and executing a domestic consequence management mission requires JTF-Civil Support to work closely with the many other Federal, state and local agencies that also respond to CBRNE situations. These agencies include, but are not limited to, the Department of Homeland Security's Federal Emergency Management Agency, the Department of Health and Human Services, and state emergency management agencies. DOD is an essential member of the Federal response community and interagency preparedness.[414]

JTF-Civil Support Mission

The mission of JTF-Civil Support is to provide command and control for Department of Defense forces deployed in support of a Lead Federal Agency (LFA) managing the consequences of a chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) incident in the United States, its territories and possessions, in order to save lives, prevent injury and provide temporary critical life support. JTF-Civil Support serves as a standing operational headquarters for USNORTHCOM.

The JTF-Civil Support mission includes, but is not limited to, the following range of activities:

- Conduct contingency planning with Federal departments and agencies.

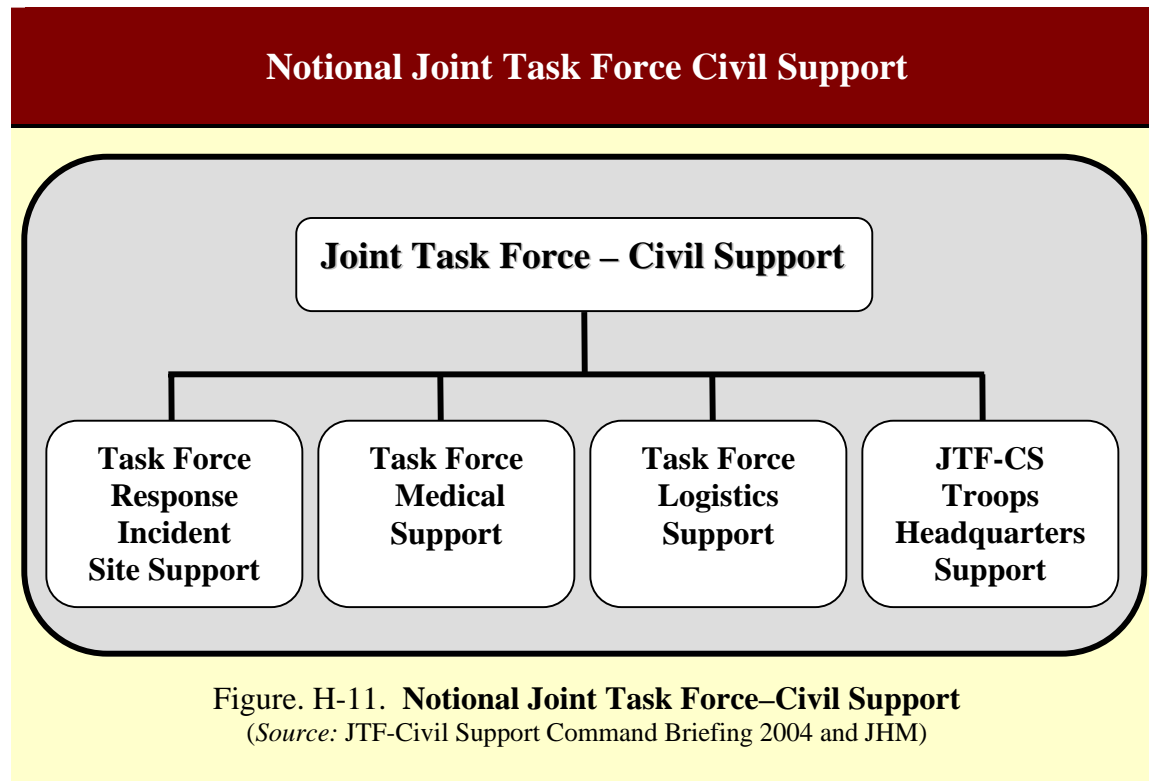- Conduct operational liaison activities with local, state and Federal departments and agencies.

---

[413] See CJCSI 3110.16, *Military Capabilities, Assets, and Units of CBRNE CM Operations*, for a sampling of DOD CBRNE consequence management type-units and agencies that may be configured in JTF-Civil Support.
[414] Joint Task Force – Civil Support [U.S. Northern Command] website; available at
http://www.jtfcs.northcom.mil; Internet; accessed 14 April 2004.

- Conduct CBRNE CM exercises within DOD and with other local, state and Federal departments and agencies.

- Conduct CBRNE CM training and exercises with DOD forces identified to conduct CBRNE CM operations.

- Conduct situational assessments following CBRNE events for the Commander in close coordination with state and Federal authorities.

- Organize, deploy, establish command and control, and redeploy DOD assigned, attached, operationally or tactically controlled forces.

- Conduct deliberate planning in support of designated National Security Special Events (NSSEs).

- Organize and provide CBRNE consequence management planning augmentation and technical support as directed.

The diagram at Figure H-11 shows the main types of task force elements that may comprise a Joint Task Force – Civil Support. This notional illustration for a response incident presents four main elements: site support, medical support, logistical support, and support for the JTF headquarters.

Notional Joint Task Force Civil Support

Joint Task Force – Civil Support

| Task Force Response Incident Site Support | Task Force Medical Support | Task Force Logistics Support | JTF-CS Troops Headquarters Support |

Figure. H-11. **Notional Joint Task Force–Civil Support**
(*Source:* JTF-Civil Support Command Briefing 2004 and JHM)

Conclusion

Terrorist groups are seeking to acquire WMD with the stated purpose of killing large numbers of U.S. people and U.S. friends and allies - without compunction and without warning.[415] The threat posed by terrorists with the intent to use weapons of mass destruction is ominous. WMD attack has several desired outcomes by terrorists. These expectations range from extensive disruption of everyday lifestyles to a more serious boding of massive damage to physical infrastructure, the economy, or mass casualties requiring long-term health care. Ultimately, a significant impact could be an intimidating psychological trauma from physical and emotional stress. Simply stated, the ***potential*** for mass injury or death, as well as mass damage or destruction, presents a compelling requirement for protective measures and increased assurance to counter public anxiety and fear.[416]

Defined in Title 18, a *Weapon of Mass Destruction (WMD)* is (1) any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, or a missile having an explosive or incendiary charge of more than one quarter ounce, or mine or device similar; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.[417]

> **"The gravest danger our Nation faces lie at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination. The United States will not allow these efforts to succeed.... History will judge harshly those who saw this coming danger but failed to act. In the new world we have entered, the only path to peace and security is the path of action."**

> George W. Bush
> President of the United States of America
> September 17, 2002

Current and potential linkages among terrorist groups and state sponsors of terrorism are particularly dangerous and require priority attention. Catastrophic incidents with CBRNE, including terrorism, will result in unprecedented levels of damage and disruption severely affecting the population, infrastructure, environment, and economy. The aftermath of such a

---

[415] HSPD-17, 1.

[416] Steven Bowman, *Weapons of Mass Destruction: The Terrorist Threat,* Congressional Research Service Report for Congress, CRS Order Code RL31332, 7 March 2002; available from http://www.fas.org/irp/crs/RL31332.pdf; Internet; accessed 15 April 2004.

[417] National Response Plan, Final Draft, 94.

catastrophic event would result in sustained national impacts over a prolonged period of time.[418] Consequence management is essential to the U.S. arsenal bearing against the WMD terrorist threat.[419]

Three principal pillars summarize the U.S. *National Strategy to Combat Weapons of Mass Destruction*: (1) counterproliferation to combat WMD use; (2) strengthened nonproliferation to combat WMD proliferation; and (3) consequence management to respond to a WMD incident.   The U.S. Government is prepared to deal with the consequences of chemical, biological, radiological, or nuclear weapon use within and outside of the United States.[420] The Department of Defense remains the greatest U.S. Federal repository of resources and subject matter expertise for responding to a chemical, biological, radiological, or nuclear incident.[421] The growing pattern of high yield explosive use adds to a macabre inventory of a terrorist bent on mass destruction effects.

As witnessed after the events of 9-11, DOD will most likely be involved in consequence management operations following a significant terrorist attack on the United States. Especially those attacks that include CBRNE.

Joint Task Force Civil Support is a ready expression of U.S. capability to respond to such incidents of chemical, biological, radiological, nuclear, and high yield explosives (CBRNE).

---

[418] National Response Plan, Final Draft, 81.
[419] HSPD-17, 7.
[420] HSPD-17, 6.
[421] Congressional Research Service, *Homeland Security: The Department of Defense's Role*, CRS Order Code RL 31615, 8.

Appendix I
Cyber Operations

Information technology (IT) and digitization are integral elements woven into the virtual fabric of today's society. Whether in our personal or professional lives, the cyber world has become dominant. In fact, as the CIA noted in a statement for the Joint Economic Committee in 2001, "Most experts agree that the IT revolution represents the most significant global transformation since the Industrial Revolution beginning in the mid-eighteenth century."[422] The increasingly indispensable nature of information technology, however, has transformed these systems into high value targets of cyber terrorists and presents a significant threat to both the military and national security.

To highlight the importance of this technology to the U.S. military, in July 2003, DOD had more than 3 million individual computers on 12,000 local area networks (LANs). [423] These interconnected systems and LANs are part of what is known as the Global Information Grid (GIG), which is the globally interconnected set of information capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel. It includes all owned and leased communications and computing systems and services, software, data, security services, and other associated services necessary to achieve information superiority.[424]

The GIG supports all DOD, National Security, and related intelligence community missions and functions in both peace and war that span the strategic, operational, tactical, and business arenas. The GIG provides capabilities from all operating locations, including bases, facilities, mobile platforms, and deployed sites; and provides interface to coalition, allied, and non-DOD users and systems.[425]

A portion of the GIG, the Defense Information System Network (DISN), is the global, end-to-end information transfer infrastructure of DOD. It provides long haul data, voice, video, and transport networks and services needed for national defense command, control, communication, and intelligence requirements, as well as corporate defense requirements.[426] Examples of the services include video teleconferencing, the Defense Switched Network (DSN), the uNclassified IP Router NETwork (NIPRNET), and the Secret IP Router NETwork (SIPRNET).

---

[422] Director of Central Intelligence, *Cyber Threat Trends and U.S. Network Security*, Statement for the Record for the Joint Economic Committee by Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, (Washington, D.C., 21 June 2001), 1; available from http://www.cia.gov/cia/public_affairs/speeches/2001/gershwin_speech_06222001.html; Internet; accessed 14 April 2004.

[423] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 3; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

[424] "Global Information Grid," Defense Information Systems Agency, Network Services (Website on line, n.d.); available from http://www.disa.mil/ns/gig.html; Internet; accessed 7 April 2004.

[425] Ibid.

[426] "Defense Information System Network," Defense Information Systems Agency, Network Services (Website on line, n.d.); available from http://www.disa.mil/ns/gig.html; Internet; accessed 7 April 2004.

Figure I-1. The Global Information Grid
(Source: Defense Information Systems Agency)

Just as the United States has capitalized on the use of computer technology, our enemies have not overlooked the fact that they must also operate in the computer age. As briefed to Congress in July 2003 by the Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command/Vice Director, Defense Information Systems Agency, the sophisticated threat to our Global Information Grid is extensive and presents a real danger to our national security. This threat includes more than 40 nation-states that have openly declared their intent to develop cyber warfare capabilities. Additionally, it includes transnational and domestic criminal organizations, hacker groups who sympathize with our [U.S.] enemies, terrorist organizations (evidenced by forensic analysis of captured computers) and insiders who support our enemies.[427]

Terrorists realize the benefits they can reap from using this technology. Equipped with a personal computer and an Internet connection, small players can somewhat level the playing field with their larger opponents in this "cyber arena." Terrorists do not have to expend large resources on a global intelligence collection organization or match the United States weapon for weapon on the battlefield to execute an operation. Terrorist groups can use cyber capabilities to assist them in planning and conducting their operations, and also to create destruction and turmoil by attacking our GIG systems and our critical infrastructures. Although many people believe terrorists only operate in the world of physical violence, many terrorist groups have well educated people and modern computer equipment to compete in

---

[427] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 3-4; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

cyberspace. Consequently, to fully understand the threat, we need to be cognizant of both sides of cyber operations—cyber support to terrorist operations and cyber-terrorism.

Cyber Support to Terrorist Operations

Terrorists recognize the benefit of cyber operations and continue to exploit information technology in every function of their operations. Macro-functions include:

Planning

Terrorists use the cyber infrastructure to plan attacks, communicate with each other, and posture for future exploitation. Employing easy-to-use encryption programs that they can easily download from the Internet, terrorists are able to communicate in a secure environment. Using steganography, they hide instructions, plans and pictures for their attacks in pictures and posted comments in chat rooms. The images and instructions can only be opened using a "private key" or code known only to the recipients. In fact, reports are that encryption has become a common tool of Muslim extremists and that it is being taught in their training camps.[428] Additionally, these encryption programs can scramble telephone conversations when the phones are plugged into a computer.[429]

Recruitment

Recruitment is the life-blood of a terrorist organization and they use multiple methods to entice new members. In addition to traditional methods, such as written publications, local prayer leaders, audio-video cassettes and CDs promoting their cause; terrorist groups also use their own websites to recruit new members. This is accomplished by providing their view of the history of their organization, its cause, and additional information to encourage potential members to join. Additionally, they often have hyperlinks to other material to encourage membership. They also use these sites to collect "donations" for the cause. Good examples of these websites include HAMAS, http://www.hamasonline.com/; Hizballah, http://www.hizbollah.org/; Revolutionary Armed Forces of Colombia (FARC), http://www.farcep.org/pagina_ingles/; and the Earth Liberation Front (ELF), http://www.earthliberationfront.com/main.shtml.

Research

Using the Internet, terrorists can tap into thousands of databases, libraries and newsgroups around the world to gather information on any subjects that they need to research. The information can be in the form of text, maps, satellite images, pictures or even video material. The use of search engines, such as Google, have made searching the Internet very easy and allows terrorists to obtain critical information located in the public domain using very simple resources. For example, by typing "Bombs" in the Google search engine, 2,870,000 references were found in 0.17 seconds. To narrow this list, typing "Bombs AND Homemade," resulted in 47,200 references being found in 0.08 seconds. Although most of these are harmless references that may just refer to news articles, many provide detailed

---

[428] Jack Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today*, 5 February 2001; available from http://www.usatoday.com/tech/news/2001-02-05-binladen.htm; Internet; accessed 6 April 2004.
[429] Ibid.

information on how to manufacture bombs. One site not only provided information on bombs, but also provided additional references on subjects such as drugs, fake IDs, fraud, lock picking, and weapons.

To highlight the importance terrorists place on research over the Internet, an al Qaeda training manual recovered in Afghanistan states: "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." After finding this manual, Secretary of Defense Donald Rumsfeld disseminated a memo to the armed services stating: "One must conclude our enemies access DoD Web sites on a regular basis."[430] The memo directed the military to purge their websites of information that could benefit our potential enemies.

Although the military has tightened up security on their sites, terrorists can still conduct research on military units. Using a search engine, they simply type in a specific organization and the search engine will provide the links if they exist. For example, typing in "Army AND Fort Hood" results in the Fort Hood home page being displayed. From this site you can still determine the entire list of units assigned to III Corps simply by opening this web page. Looking at the Fort Bragg web site, you can quickly obtain a map of the installation, the schedule for the installation shuttle bus, and a copy of the official telephone directory, which provides all of the units on the installation. You can also find out other critical information on the military, such as every Army and Air Force airfield in the United States, and the location of military ammunition depots throughout CONUS.

Terrorists can also use the Internet to research information on the critical infrastructure of the United States. In the fall of 2001, police found a pattern of surveillance by Middle East and South Asia unknown browsers against Silicon Valley computers used to manage Bay Area utilities and government offices. As the FBI became involved, the trail revealed even broader surveillance, casing sites nationwide. Routed through telecommunication switches in Saudi Arabia, Indonesia, and Pakistan, surveillance was conducted on emergency telephone systems, electrical generation and transmission facilities, water storage and distribution systems, nuclear power plants, and gas facilities.[431]

Unfortunately, using the convenience of the Internet, terrorists can virtually research any subject, to include information on potential targets, without ever leaving the safety of their locales overseas or within the United States.

Propaganda

As Christopher Harmon states in his book, *Terrorism Today*, "Propaganda is a veritable terror group standard."[432] Terrorist organizations depend on the backing of a broad base of support for both recruiting and funding. They use propaganda to discredit their enemy while making themselves look good. Earlier terrorist groups published newspapers and leaflets to spread

---

[430] Kevin Poulsen, "Rumsfeld Orders .mil Web Lockdown," *The Register*, 17 January 2003; available from http://www.theregister.co.uk/2003/01/17/rumsfeld_orders_mil_web_lockdown; Internet; accessed 8 April 2004.
[431] Bartom Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washingtonpost.com,* 27 June 2002; available from http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; accessed 12 April 2004.
[432] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 55.

their propaganda. Although this form of media is still widely used, terrorist groups are now using the Internet. Most radical groups of international significance operate Internet sites. These groups post articles supporting their agendas on these sites, which make them instantly available to the worldwide cyber community. Radical Islam in particular makes use of propaganda to enlist the support of their own public for jihad and to demoralize the enemy. The statement from the Hizballah website is an example of some of their propaganda.
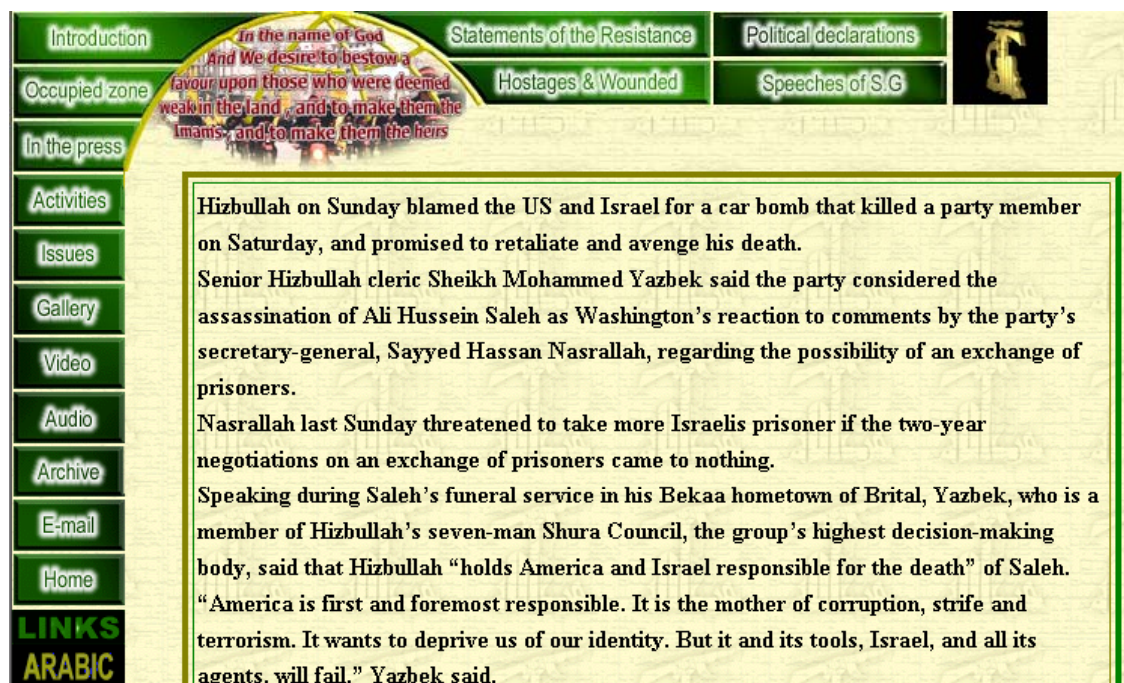
Figure I-2: Hizballah Website Example

Cyber-Terrorism

Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves. Cyber-terrorism is a new and somewhat nebulous concept, with debate as to whether it is a separate phenomenon, or just a facet of information warfare practiced by terrorists. Even for those that believe cyber-terrorism is a separate phenomenon, the boundaries often become blurred between information warfare, computer crime, online social activism and cyber-terrorism.

Cyber-terrorism differs from other improvements in terrorist technology because it involves offensive information technology capabilities, either alone or in combination with other forms of attack. Some examinations of cyber-terrorism focus on the physical destruction of information hardware and software, or physical damage to personnel or equipment using information technology as the medium. Examples of this approach would include the chaos and destruction caused by disrupting a nation's air traffic control system, crashing two trains together by overriding the railroad signal and switching system, or the loss to the economy by blocking and falsifying commercial communications.

One common aspect is that organizations trying to attack using information technology will more than likely want to keep the information network up, or at least limit their destruction or disruptions to discrete portions of the network. For a true "cyber-terrorist," the network is the method of attack. It is the weapon, or at the least, the medium through which an attack is delivered. Information warfare of this sort requires that messages and computer commands are transmitted, programs and malicious software be emplaced, fraudulent transactions take place, and information be available for exploitation. Defacing websites, crashing portions of a target network, accessing enemy information, denying network access to other groups, manipulating financial confidence and causing panic exemplify this warfare. Still, they require that the target network remain more or less intact. A terrorist group could crash a network through physical destruction or technological attack, but only a group whose perceived gains would offset their loss of information, communication, and other capabilities would do this.[433]

Outside of computer networks, communications networks can also be targeted for destruction, disruption, or hijacking. This has a direct impact on the military and the government since a large percentage of the GIG is dependent on commercial telephone links and the Internet. Destructive and disruptive attacks upon communication networks would likely be supporting operations designed to increase the effectiveness of physical attacks. Hijacking, or taking control of a communication network might support another operation, or be attempted for it's own impact. Dissident factions have already substituted their own satellite TV signals for state controlled broadcasting.[434] Terrorists could exploit such capabilities to bypass mainstream media restraint in covering particularly shocking actions, or to demonstrate their power and capability to challenge their enemies.

Other views of cyber terror stress the manipulation, modification, and destruction of non-physical items such as data, websites, or the perceptions and attitudes this information can influence. Attacks that would destroy electronic records of financial transactions, or permit large-scale electronic theft would cause significant economic damage to a country, but not truly "exist" in the physical world. Changing the information or appearance of an enemy's official web page allows the terrorist to spread negative perceptions or false information without physical intrusion.

Currently, DOD does not have a definition of cyber-terrorism, but does define cyberspace as: "The notional environment in which digitized information is communicated over computer networks."[435] In the Federal Government, the FBI describes cyber-terrorism as: "Cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda."[436] Another definition by Kevin Coleman, a former chief strategist at Netscape who

---

[433] John Arquilla and David Ronfeldt, ed., *Networks and Netwars* (Santa Monica: RAND, 2001): 5.

[434] "Chinese Satellite TV Hijacked by Falun Gong Cult," *People's Daily Online*, 9 July 2002; available from http://english.peopledaily.com.cn/200207/08/eng20020708_99347.shtml; Internet; accessed 27 November 2002.

[435] Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 17 December 2003.

[436] Harold M. Hendershot, "CyberCrime 2003 – Terrorists' Activity in Cyberspace" (Briefing slides from the Cyber Division, Federal Bureau of Investigation, Washington, D.C.): 12; available from http://www.4law.co.il/L373.pdf; Internet; accessed 6 April 2004.

writes a Homeland Security focused column for *Directions* magazine is: "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."[437]

These definitions spotlight the fact that cyber-terrorism is a serious threat. In the first half of 2002, there were more than 180,000 Internet based attacks on business and these attacks are increasing at an annual rate above 60%. Additionally, it is estimated that the reported incidents may represent only 10% of the actual total. A research study conducted by the Computer Crime Research Center in 2002 reported that 90% of respondents detected computer security breaches within the previous twelve months.[438] In the Department of Defense, the speed and complexity of attacks are increasing. The Defense Information Systems Agency estimated in 1996 that DOD IT systems were attacked about 250,000 times per year and the GAO reported in the same year that only about 1 in 500 attacks were detected and reported.[439] In 2002, DOD successfully defended against 50,000 intrusion attempts to gain root access to the GIG. By June 2003, there were over 21,000 attempts.[440]

Objectives of Cyber Attack

When analyzing the objectives of a cyber attack and the ultimate outcome the attack may have, the effects of cyber attack align generally into four areas. The first three effects listed below address the impact on the actual IT systems themselves, [441] whereas the last effect addresses the impact of using the IT system for physical destructive purposes.

- Loss of Integrity. System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

- Loss of Availability. If a mission-critical IT system is attacked and rendered unavailable to its end users, the organization's mission will most likely be affected. Loss of system

---

[437] Kevin Coleman, "Cyber Terrorism," *Directions Magazine,* 10 October 2003, 1; available from http://www.directionsmag.com/article.php?article_id=432; Internet; accessed 15 March 2004.

[438] Ibid., 2-3.

[439] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84, (Washington, D.C., 22 May 1996), 1; available from http://www.fas.org/irp/gao/aim96084.htm; Internet; accessed 12 April 2004.

[440] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 9; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

[441] Department of Commerce, National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems,* NIST Special Publication 800-30, by Gary Stoneburner, Alice Goguen, and Alexis Feringa, (Washington, D.C., 2001): 22; available from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf; Internet; accessed 12 April 2004.

functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

- Loss of Confidentiality. System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

- Physical Destruction. Physical destruction refers to the ability to create actual physical harm or destruction through the use of IT systems. Much of our critical infrastructure, such as transportation, power, and water companies are operated with networks of computer-controlled devices known as supervisory control and data acquisition (SCADA) systems. These systems can be attacked and used to cause operations to malfunction, such as the release of water from a dam or switching the tracks on a railroad to create a collision. There have also been concerns that a terrorist could take control of the air traffic control system and cause aircraft to crash. Fortunately these specific scenarios have not occurred, and there are normally sufficient manual checks and overrides that help prevent this type of failure. However, the possibility of taking over a SCADA system is real. There was a case in 2001 where an individual used the Internet, a wireless radio, and stolen control software to release up to 1 million liters of sewage into the river and coastal waters of Queensland, Australia. The individual had attempted to access the system 44 times, prior to being successful in his 45th attempt, without being detected.[442] This example does indicate that individuals with the proper tools and knowledge can bypass security in public utilities or other organizations using SCADA systems.

Actors

Not every individual or group who uses information technology to further their agenda or attack their opponents are necessarily cyber terrorists. However, it can often be difficult to determine if an attack is originating from terrorists or from high school students with the technical expertise to access your system. It often becomes a judgment call on what is truly cyber-terrorism and what is just hacking. There are various categories of attackers that the military may be faced with in the cyber arena.

- Hackers: These are advanced computer users who spend a lot of time on or with computers and work hard to find vulnerabilities in IT systems. Some hackers, known as Whitehat Hackers, look for vulnerabilities and then work with the vendor of the affected system to fix the problem. The typical hacker, though, is often referred to as a Blackhat Hacker. They are the individuals who illegally break into other computer systems to damage the system or data, steal information, or cause disruption of networks for personal motivations, such as monetary gain or status. However, they generally lack the motivation to cause violence or severe economic or social harm.

---

[442] Robert Lemos, "What are the Real Risks of Cyberterrorism?" *ZDNet,* 26 August 2002, 4; available from http://zdnet.com.com/2102-1105_2-955293.html; Internet; accessed 6 April 2004.

An example of the systems hackers can access was demonstrated in 1998. Two teenage hackers accessed computers at Lawrence Livermore National Laboratory, the U.S. Air Force, and other organizations. After being caught by the FBI, the teenagers pleaded guilty to illegally accessing restricted computers, using "sniffer" programs to intercept computer passwords, and reprogramming computers to allow complete access to all of their files. They also inserted "backdoor" programs in the computers to allow themselves to re-enter at will.[443]

A concern beyond just gaining access to a system is what hackers may do with information that they steal from the military. In November 1998, the Detroit News reported that a member of Harkat-ul-Ansar, a militant Pakistani group, tried to buy military software from hackers who had stolen it from DOD computers.[444]

- "Hactivists:" These are combinations of hackers and activists. They usually have a political motive for their activities, and identify that motivation by their actions, such as defacing opponents' websites with counter-information or disinformation. Alone, these actions bear the same relation to cyber-terrorism that theft, vandalism, or graffiti do to mundane physical terrorism; they may be an unrelated activity, or a supporting piece of a terrorist campaign.

An example of this type activity occurred following the inadvertent bombing of the Chinese embassy in Belgrade during the 1999 NATO bombing campaign in Yugoslavia when pro-Beijing Chinese hackers conducted mass cyber protests against U.S. government Web sites in response to this accident. This type activity occurred again in May 2001 when Chinese protesters defaced or closed over 100 sites in the U.S., after a Chinese fighter jet collided with a U.S. reconnaissance plane off the Chinese coast.

- Computer Criminals: Criminals have discovered they can exploit computer systems, primarily for financial gain. Computer extortion is a form of this type crime. An example is the case of media titan Michael Bloomberg. His corporation was hacked into by two suspects who demanded two hundred thousand dollars from Bloomberg in "consulting fees" in order for them to keep quiet on how they compromised Bloomberg's computer system.

Another example deals with gaining unauthorized access to government computers and obtaining information for financial gain. In September 2003, an individual was in a conspiracy to access military, government and private sector computers. The indictment alleged that the defendant was the president of a computer security company and he was trying to gain unauthorized access to government and military computers, copy computer files and take these files to the media in order to generate public visibility for his company. He thought this would lead to new clients and increased profits. According to the indictment, the conspirators possessed government files belonging to the National

---

[443] Andrew Quinn, "Teen Hackers Plead Guilty to Stunning Pentagon Attacks," Reuters, 31 July 1998, 1; available from http://www.geocities.com/Area51/Shadowlands/6583/project395.html; Internet; accessed 14 April 2004.
[444] Congress, House, Armed Services Special Oversight Panel on Terrorism, *Cyberterrorism*, Testimony by Dorothy E. Denning, Georgetown University, (Washington, D.C., 23 May 2000): 3; available from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Internet; accessed 9 April 2004.

Aeronautics and Space Administration (NASA), United States Army, United States Navy, Department of Energy and National Institutes of Health.[445]

- Industrial Espionage: Industrial espionage has a long history in our industrialized society and there is no question that with today's reliance on computer systems and networks to plan, document, and store research data; industrial espionage has added the electronic medium to its list of methods of operation. These industrial spies may be government sponsored or affiliated, from commercial organizations, or private individuals. Their purpose may be to discover proprietary information on financial or contractual issues, or to acquire classified information on sensitive research and development efforts.

  Although industrial espionage is normally associated with civilian corporations, it can have a direct impact on the military as well. As stated by the Defense Security Service (DSS) in a 2002 report, U.S. military critical technologies are the most sought after in the world.[446] The espionage may be directed against a defense contractor; against DOD's military research, development, test, and evaluations community; or against DOD's acquisition program offices. To demonstrate the assault against military technology, DSS received reports of suspicious activities concerning defense technology from sources in 75 countries in 2001. This activity covered every militarily critical technology category, with the highest interest being information systems, sensors and lasers, armaments and energetic materials, aeronautic systems, and electronics.[447]

- Insiders: Although IT professionals do everything possible to secure their systems from outsiders; there is always the threat of an insider with authorized access to a system conducting an attack. These insiders may be disgruntled employees working alone, or they may be working in concert with other terrorists to use their access to help compromise the system.

  An example occurred in July 1997, when a U.S. Coast Guard employee used her insider knowledge and another employee's password and logon identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency employees over 1800 hours to recover and reenter the lost data.

- Consultants/contractors: Another concern is the practice by many organizations to use outside contractors to develop software systems. This often provides these contractors with the access required to engage in cyber-terrorism.

  In March 2000, Japan's Metropolitan Police Department reported that they had procured a software system to track police vehicles that had been developed by Aum Shinryko. This is the cult that released sarin gas in the Tokyo subway in 1995. The police discovered that

---

[445] Department of Justice, U.S. Attorney Southern District of California, Press Release, *President of San Diego Computer Security Company Indicted in Conspiracy to Gain Unauthorized Access into Government Computers*, (San Diego, CA, 29 September 2003): 1; available from http://www.usdoj.gov/criminal/cybercrime/okeefeArrest.htm; Internet; accessed 12 April 2004.

[446] Department of Defense, Defense Security Service, *Technology Collection Trends in the U.S. Defense Industry 2002* (Alexandria, VA, n.d.), 1; available from http://www.wright.edu/rsp/Security/TechTrends.pdf; Internet; accessed 19 April 2004.

[447] Ibid., 2-3.

the cult had received classified tracking data on 115 of the vehicles. Additionally, the cult had developed software for 80 Japanese firms and 10 government agencies. One of several concerns is that they had installed a Trojan horse in the systems to launch or facilitate cyber terrorist attacks at a later date.[448]

- Terrorists: Although there have been no major cyber attacks caused by terrorist groups that have taken lives or caused severe physical destruction, some government experts believe that terrorists are at the point where they may be able to use the Internet as a direct instrument to cause casualties, either alone or in conjunction with a physical attack. In fact, the FBI's director of the National Infrastructure Protection Center stated in 2002, "The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders' 911 system or on the power grid."[449]

  The Cyber Division of the FBI states that in the future, cyber-terrorism may become a viable option to traditional physical acts of violence due to:[450]

    - Anonymity
    - Diverse targets
    - Low risk of detection
    - Low risk of personal injury
    - Low investment
    - Operate from nearly any location
    - Few resources are needed

The following table from the National Institute of Standards and Technology summarizes threats to IT systems, including the source, their motivation, and actions.[451]

---

[448] Ibid., 3.

[449] Bartom Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washingtonpost.com,* 27 June 2002; available from http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; accessed 12 April 2004.

[450] Harold M. Hendershot, "CyberCrime 2003 – Terrorists' Activity in Cyberspace" (Briefing slides from the Cyber Division, Federal Bureau of Investigation, Washington, D.C.): 7; available from http://www.4law.co.il/L373.pdf; Internet; accessed 6 April 2004.

[451] Department of Commerce, National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems,* NIST Special Publication 800-30, by Gary Stoneburner, Alice Goguen, and Alexis Feringa, (Washington, D.C., 2001): 14; available from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf; Internet; accessed 12 April 2004.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	. Hacking . Social engineering . System intrusion, break-ins . Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	. Computer crime (e.g., cyber stalking) . Fraudulent act (e.g., replay, impersonation, interception) . Information bribery . Spoofing . System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	. Bomb/Terrorism . Information warfare . System attack (e.g., distributed denial of service) . System penetration . System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	. Economic exploitation . Information theft . Intrusion on personal privacy . Social engineering . System penetration . Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	. Assault on an employee . Blackmail . Browsing of proprietary information . Computer abuse . Fraud and theft . Information bribery . Input of falsified, corrupted data . Interception . Malicious code (e.g., virus, logic bomb, Trojan horse) . Sale of personal information . System bugs . System intrusion . System sabotage . Unauthorized system access

Table I-1. Human Threats – Threat-Source, Motivation, and Threat Actions

Tools of Cyber Attacks

There are a myriad of tools that cyber terrorists will use to accomplish their objectives. Some of these are:

- Backdoor: This is used to describe a back way, hidden method, or other type of method of by passing normal security in order to obtain access to a secure area. It is also referred to as a trapdoor. Sometimes backdoors are surreptitiously planted on a network element; however, there are some cases where they are purposely installed on a system. An example of this is the craft interface. This interface is on network elements and is designed to facilitate system management, maintenance, and troubleshooting operations by technicians, called craft personnel. The craft interface allows the technician to access the equipment on site, or in many cases, access it via remote terminal. Actions they can conduct include: [452]

  - Initial turn–up of network elements and/or systems
  - Trouble verification
  - Repair verification
  - Monitor network element (NE) performance
  - Update NE software and hardware
  - Manual control of NE
  - Remote inventory

  Security for these interfaces is normally via userids and passwords. Unfortunately, passwords are often the weakest link in a computer security scheme because password cracking tools continue to improve and the computers used to crack passwords are more powerful than ever. Network passwords that once took weeks to crack can now be cracked in hours.

  Although the craft interface allows the service provider access to conduct maintenance on the equipment, many vendors build back doors to have access to these interfaces so they can also remotely troubleshoot equipment. Unfortunately, this means a technician from outside the organization is able to gain access to the system and could facilitate cyber terrorist activities.

- Denial of Service Attacks (DOS): A DOS attack is designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash. An even more effective DOS is the distributed denial of service attack (DDOS). This involves the use of numerous computers flooding the target simultaneously. Not only does this overload the target with more requests, but having the DOS from multiple paths makes backtracking the attack extremely difficult, if not impossible. Many times worms are planted on computers to create zombies that allow the attacker to use these machines as unknowing participants in the attack. To highlight the impact of these type attacks, in February 2000, DOS attacks against Yahoo, CNN, eBay and other e-commerce sites were estimated to have caused over a billion dollars in

---

[452] "NE-NE Remote Login Initial Solution Evaluation Criteria," *SONET Interoperability Forum* Document Number SIF-RL-9605-043-R4, (12 June 1996): 4; available from http://www.atis.org/pub/sif/approved/sif96008.pdf; Internet; accessed 9 April 2004.

losses.[453] DOS attacks have also been directed against the military. In 1999, NATO computers were hit with DOS attacks by hactivists protesting the NATO bombing in Kosovo.

- E-mail Spoofing: E-mail spoofing is a method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source. This method is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords). For example, e-mail could be sent claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information.

- IP Address Spoofing: A method that creates Transmission Control Protocol/Internet Protocol (TCP/IP) packets using somebody else's IP address. Routers use the "destination IP" address to forward packets through the Internet, but ignore the "source IP" address. This method is often used in DDOS attacks in order to hide the true identity of the attacker.

- Keylogger: A software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the actual keys being typed, a user can easily obtain passwords and other information the computer operator may not wish others to know.

- Logic bomb: A program routine that destroys data by reformatting the hard disk or randomly inserting garbage into data files. It may be brought into a computer by downloading a public-domain program that has been tampered with. Once it is executed, it does its damage immediately, whereas a virus keeps on destroying.

- Physical Attacks: This involves the actual physical destruction of a computer system and/or network. This includes destroying transport networks as well as the terminal equipment.

- Sniffer: A program and/or device that monitors data traveling over a network. Although sniffers are used for legitimate network management functions, they also are used during cyber attacks for stealing information, including passwords, off a network. Once emplaced, they are very difficult to detect and can be inserted almost anywhere.

- Trojan Horse: A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed performs a function in the background such as allowing other users to have access to your computer or sending information from your computer to other computers.

- Viruses: A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. There are different types of viruses. Some of these are:

---

[453] Congress, House, Armed Services Special Oversight Panel on Terrorism, *Cyberterrorism*, Testimony by Dorothy E. Denning, Georgetown University, (Washington, D.C., 23 May 2000), 1; available from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Internet; accessed 9 April 2004.

- Boot Sector Virus: Infects the first or first few sectors of a computer hard drive or diskette drive allowing the virus to activate as the drive or diskette boots.
- Companion Virus: Stores itself in a file that is named similar to another program file that is commonly executed. When that file is executed the virus will infect the computer and/or perform malicious steps such as deleting your computer hard disk drive.
- Executable Virus: Stores itself in an executable file and infects other files each time the file is run. The majority of all computer viruses are spread when a file is executed or opened.
- Overwrite Virus: Overwrites a file with its own code, helping spread the virus to other files and computers.
- Polymorphic Virus: Has the capability of changing its own code allowing the virus to have hundreds or thousands of different variants making it much more difficult to notice and/or detect.
- Resident Virus: Stores itself within memory allowing it to infect files instantaneously and does not require the user to run the "execute a file" to infect files.
- Stealth Virus: Hides its tracks after infecting the computer. Once the computer has been infected the virus can make modifications to allow the computer to appear that it has not lost any memory and or that the file size has not changed.

- Worms: A destructive software program containing code capable of gaining access to computers or networks and once within the computer or network causing that computer or network harm by deleting, modifying, distributing, or otherwise manipulating the data.

- Zombie: A computer or server that has been basically hijacked using some form of malicious software to help a hacker perform a Distributed Denial Of Service attack (DDOS).

Cyber Threat to U.S. Critical Infrastructures

Several studies examining the cyber threat have shown that critical infrastructures are potential targets of cyber terrorists. These infrastructures make extensive use of computer hardware, software, and communications systems. However, the same systems that have enhanced their performance potentially make them more vulnerable to disruption by both physical and cyber attacks to these IT systems. These infrastructures include: [454]

- Energy systems
- Emergency services
- Telecommunication
- Banking and finance
- Transportation
- Water system

---

[454] Department of the Treasury, Office of the Comptroller of the Currency, *Infrastructure Threats from Cyber-Terrorists*, OCC Bulletin 99-9, (Washington, D.C., 5 March 1999), 2; available from http://www.occ.treas.gov/ftp/bulletin/99-9.txt; Internet; accessed 6 April 2004.

A quick review of the automation used in the electric power industry demonstrates the potential vulnerabilities to our critical infrastructures. The electrical industry has capitalized on computer technology for improved communication and automation of control centers, substations and remote protection equipment. They use a host of computer-based equipment including SCADA systems; substation controllers consisting of programmable logic controllers, remote terminal units, data processing units and communication processors; and intelligent electronic devices consisting of microprocessor-controlled meters, relays, circuit breakers, and circuit reclosers. If unauthorized personnel gain cyber access to these systems, any alterations to settings or data can have disastrous consequences similar to physical sabotage, resulting in widespread blackouts.[455]

There have been many documented attacks against this infrastructure from hackers and criminals. As an example, FBI agents arrested a Louisiana man in February 2004 for sending an e-mail to certain users of a WebTV service that, once opened, reprogrammed their computers to dial "9-1-1" instead of a local Internet access telephone number. The 9-1-1 calls caused by the e-mail resulted in the dispatch of police in locations from New York to California.[456]

Another example occurred in New York in 1997. A juvenile accessed the components of the phone system operated by NYNEX. Several commands were sent that disrupted the telephone service to the Federal Aviation Administration tower at the Worcester Airport, to the Worcester Airport Fire Department, and to other related entities such as airport security, the weather service, and various private airfreight companies. As a result of this disruption, the main radio transmitter and the circuit, which enabled aircraft to send an electronic signal to activate the runway lights on approach, were disabled. This same individual then accessed the loop carrier system for customers in and around Rutland, Massachusetts and sent commands that disabled the telephone service, including the 911 service, throughout the Rutland area.[457]

Although there have been no major terrorist attacks to these critical infrastructure systems to date, there is evidence that terrorist groups have been conducting surveillance on them. As stated earlier in this section under "Research," police have found a pattern of surveillance by unknown browsers located in the Middle East and South Asia against emergency telephone systems, electrical generation and transmission facilities, water storage and distribution systems, nuclear power plants, and gas facilities.

Although these systems fall within the civilian sector, the military is highly dependent on all of these critical functions and would be directly impacted if they were successfully attacked. Consider the impact on unit deployment if a successful cyber attack, or a combination of cyber and physical attack, is conducted against our critical infrastructure during movement—

---

[455] Paul Oman, Edmund Schweitzer, and Jeff Roberts, "Protecting the Grid from Cyber Attack Part I: Recognizing Our Vulnerabilities," *Utility Automation and Engineering T&D*, November 2001; available from http://uaelp.pennnet.com; Internet; accessed 24 June 2004.

[456] Department of Justice, U.S. Attorney, Northern District of California, Press Release, *Louisiana Man Arrested for Releasing 911 Worm to WebTV Users*, (San Francisco, CA, 19 February 2004), 1; available from http://www.usdoj.gov/criminal/cybercrime/jeansonneArrest.htm; Internet; accessed 12 April 2004.

[457] Congress, Senate, Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, *Cyber Terrorism*, Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, (Washington, D.C., 24 February 2004), 3; available from http://www.fbi.gov/congress/congress04/lourdeau022404.htm; Internet; accessed 15 April 2004.

- Disruption of the rail system could severely impact movement of equipment to a port of embarkation.
- A successful attack against a power substation could halt loading operations at the port.
- A successful attack against the telecommunications systems would directly impact the command and control of the operations.

Cyber Threat to the Military

As discussed at the beginning of this appendix, the military is linked together through the Global Information Grid, and the computers and computer networks comprising the GIG are likely targets for cyber terror. Although many people may think that the military's only vulnerability is to command and control systems, it is important to realize that the Department of Defense uses IT systems for a number of functions, in both peace and war. These include:[458]

- Commercial transactions
- Payrolls
- Sensitive research data
- Intelligence
- Operational plans
- Procurement sensitive source selection data
- Health records
- Personnel records
- Weapons systems maintenance records
- Logistics operations

In addition to the day-to-day operations in DOD that encompass the above functions, a current operational example of the military's reliance on the GIG is Operation Iraqi Freedom. In 2003, unclassified testimony to the House Armed Services Subcommittee on Terrorism, Unconventional Threats, and Capabilities by the Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command/Vice Director, Defense Information Systems Agency stated that deployed forces used 50 times more bandwidth per person during Operation Iraqi Freedom than during Operation Desert Storm. The GIG was used for collaborative command and control across the globe, and concurrent planning was used extensively to execute missions. Additionally, Predator aircraft used in theater to collect intelligence were controlled remotely from CONUS and the collected intelligence was analyzed in real-time.[459]

---

[458] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84, (Washington, D.C., 22 May 1996), 7; available from http://www.fas.org/irp/gao/aim96084.htm; Internet; accessed 12 April 2004.

[459] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 7-8; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

For U.S. military forces, likely "cyber terror" threats include attempts to overload data transmission and information processing capabilities. Physical destruction of some communications nodes, combined with decoys, false chatter, and deception to overload the remainder could significantly slow the ability to assess and respond to threats. Another threat is the use of unsecured personal information to target service members or their families for physical and electronic harassment campaigns. This technique has found widespread use amongst single-issue terrorists. These terrorists make phone numbers, addresses, and any other available personal information public via the Internet; and urge sympathizers or proxies to threaten and harass service members, their families, and associates, vandalize their property, or steal their identity. This could easily erode morale and inflict uncertainty and fear throughout the military community. The Provisional Irish Republican Army, who employed contract hackers to obtain home addresses of law enforcement and intelligence officers, has demonstrated this tactic. This information was used to develop plans to kill the officers if the British government did not meet terms for a cease-fire.[460]

A major threat to the military deals with the fact that a large percentage of the Global Information Grid is dependent upon commercial telecommunications links and the Internet, which are not controlled by DOD.[461] For instance, Sprint is one of the many carriers that provides the communications backbone to transport DOD data. Sprint must develop software systems to manage their network infrastructure; however, they do not have total control of who develops this software. In September 2003, Sprint announced that they were outsourcing software development, computer coding, and other related tasks to EDS and IBM.[462] A March 2004 report in *BusinessWeek online*; however, shows that these two companies are hiring offshore programmers to complete their work.[463] The question that arises is who is developing the software for them? Reviews of the companies that provide offshore development indicates over 40 countries provide this service, to include numerous Eastern European countries, China, Pakistan, and Russia. India is by far, though, the country that provides the majority of this work. One concern is how tight is their security and how well do they conduct background investigations of personnel working on products that will eventually support DOD systems? Similar to the case in Japan where Aum Shinryko developed software for the police department, it is not unreasonable to assume that malicious software or backdoors could be planted into Sprint's systems that could ultimately impact the military.

There have been many examples of attacks on the Defense Department's IT systems. Between April 1990 and May 1991, hackers from the Netherlands penetrated computer systems at 34 Defense sites. The hackers were able to access directories, read e-mail, and

---

[460] Congress, House, Armed Services Special Oversight Panel on Terrorism, *Cyberterrorism*, Testimony by Dorothy E. Denning, Georgetown University, (Washington, D.C., 23 May 2000), 3; available from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Internet; accessed 9 April 2004.

[461] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 5; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

[462] "Sprint Inks Outsouring Pacts with EDS, IBM," *Dallas Business Journal,* (16 September 2003); available from http://www.bizjournals.com/dallas/stories/2003/09/15/daily21.html; Internet; accessed 9 April 2004.

[463] "Software - Programming Jobs are Heading Overseas by the Thousands. Is there a Way for the U.S. to Stay on Top?" *BusinessWeek online*, 1 March 2004; available from http://businessweek.com/magazine/content/04_09/b3872001_mz001.htm; Internet; accessed 9 April 2004.

modify systems to obtain full privileges allowing them future access to the systems. Investigation into the unauthorized access indicated the hackers were searching the messages for key words, such as nuclear, weapons, missile, Desert Shield, and Desert Storm. The hackers also copied and stored military data on systems at major U.S. universities.[464]

More recently, an unemployed computer system administrator living in London, England hacked into nearly 100 different systems belonging to the U.S. Army, U.S. Navy, U.S. Air Force, the Pentagon, and NASA over a year period ending in March 2002. After gaining access to the various systems, he deleted user accounts and critical system files, copied files containing usernames and encrypted passwords, and installed tools used for obtaining unauthorized access to computers.[465] In one of these attacks, a network of 300 computers at a Naval weapons station was shut down for a week.[466]

The Department of Defense (DOD) has recognized the cyber threat to its systems for years. However, in 1998 DOD formally established Joint Task Force-Computer Network Defense to combat these threats. This was a result of two key factors. First, National Security Agency personnel were able to inflict, through simulation, a significant amount of damage to Defense networks during Exercise Eligible Receiver 97. This exercise involved DOD, Joint Staff, all the Armed Forces, the Defense and Central Intelligence Agencies, various combatant commands, and the Departments of State, Justice, and Transportation.[467]

The second factor occurred in February 1998, when a number of computer attacks were detected which targeted U.S. military computers worldwide. These attacks appeared to be originating from the Middle East and were initiated as the U.S. was preparing for possible military action against Iraq. The concern was that the attacks were being conducted by Iraq. An interagency investigation was quickly conducted and found that the attackers were two California teenagers and an 18-year old Israeli mentor. Although no classified systems were compromised, the security breaches could have been used to disrupt DOD information flow during possible combat operations in the Middle East. [468]

In October 2002, Joint Task Force-Computer Network Defense was re-designated Joint Task Force-Computer Network Operations (JTF-CNO) and was assigned to the U.S. Strategic Command. It includes components from all four Armed Services and the Defense Information System Agency's Computer Emergency Response Team. The task force has two missions: Computer Network Defense (CND) and Computer Network Attack (CNA). The CND mission is to defend DOD computer networks and systems from

---

[464] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84, (Washington, D.C., 22 May 1996), 16-17; available from http://www.fas.org/irp/gao/aim96084.htm; Internet; accessed 12 April 2004.
[465] Department of Justice, U.S. District Court for the Eastern District of Virginia, Alexandria Division, Indictment, *United States of America v. Gary McKinnon*, (Alexandria, VA, November 2002), 2-3; available from http://news.findlaw.com/hdocs/docs/cyberlaw/usmck1102vaind.pdf; Internet; accessed 16 April 2004.
[466] "U.S. Officials Charge Briton for Hacking Pentagon," *Asian School of Cyber Laws,* November 2002, 1; available from http://www.asianlaws.org/cyberlaw/archives/11_02_penta.htm; Internet; accessed 16 April 2004.
[467] "Eligible Receiver," *Global Security.org*, 9 June 2002; available from http://www.globalsecurity.org/military/ops/eligible-receiver.htm; Internet; accessed 24 June 2004.
[468] Colin Robinson, *Military and Cyber-Defense: Reactions to the Threat* (Washington: Center for Defense Information Terrorism Project, 2002), 1-2; available from http://www.cdi.org/terrorism/cyberdefense-pr.cfm; Internet; accessed 24 June 2004.

any unauthorized event, such as probes, scans, virus incidents, or intrusions. The CNA mission is to coordinate, support, and conduct computer network attack operations, at the direction of the President, in support of regional and national objectives.[469]

Conclusion

Although many of the current weaknesses in IT systems can be fixed, ever-evolving IT capabilities will continue to challenge cyber security and information assurance. Additionally, as one system is fixed, other vulnerabilities are often found. Even if the actual technology used in a system has excellent security, the system is often configured or used in ways that open it up for attack. Additionally, insiders can use their access to support the cyber terrorists to bypass security.[470]

As an example of how fast the cyber threat changes, the Melissa virus that infected networks in 1999 took weeks to have an effect. However, the Code Red worm that infected the Internet in July 2001 took only hours to flood the airways, while the Slammer worm that appeared in January 2003 took only minutes to infect thousands of hosts throughout the world. To further demonstrate the complexity of attacks, it took Code Red 37 minutes to double in size, but only took Slammer 8.5 seconds to do the same. In fact it took the Slammer worm only 10 minutes to infect 90 percent of vulnerable hosts.[471]

Clearly, attacks in cyberspace will continue in the future. Cyber terrorists will try to capitalize on known weaknesses and continue dedicated research and mining to discover new vulnerabilities in our systems. As stated in an al Qaeda article in February 2002, "Despite the fact that the jihadi movements prefer at this time to resort to conventional military operations, jihad on the Internet from the American perspective is a serious option for the movements in the future for the following reasons:

- First: Remote attacks on Internet networks are possible in complete anonymity.
- Second: The needed equipment to conduct attacks on the Internet does not cost much.
- Third: The attacks do not require extraordinary skill.
- Fourth: The jihadi attacks on the Internet do not require large numbers [of people] to participate in them."[472]

---

[469] "Joint Task Force-Computer Network Operations," (Offutt Air Force Base: U.S. Strategic Command Fact Sheet, 2003); available from http://www.stratcomaf.mil/factsheetshtml/jtf-cno.htm; Internet; accessed 25 June 2004.

[470] Ibid., 3.

[471] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 9; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

[472] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 36, quoting Abu 'Ubeid al-Qurashi, "The Nightmares of America, 13 February 2002.

Appendix J
Case Studies of Terrorism

…War has been waged on us [USA] by stealth and deceit and murder. This nation is peaceful, but fierce when stirred to anger. The conflict has begun on the timing and terms of others. It will end in a way, and at an hour, of our choosing.

George W. Bush
President of the United States of America
September 14, 2001

Introduction

General. This appendix presents a sampling of foreign and domestic terrorist incidents against the United States of America. Using an abridged case study methodology, analysis approaches each case from a "Threats" adversary viewpoint. Assessment provides observations on terrorist effectiveness in a contemporary operational environment.

"Constants and variables" are U.S. Army doctrinal terms of reference that describe today's operating environment. To recognize the conditions, circumstances, and influences that effect employment of terrorist acts, analysis includes constants or factors of the contemporary operational environment, as well as critical variables that define a specific operational situation.[473]

Using open source material, this case study series provides an appreciation of how much information is readily available to friend and foe in understanding the tactics, techniques, and procedures of a terrorist operation. Combined with situational awareness, U.S. military forces can better deter, dissuade, or deny terrorists in the ability to achieve terrorist acts and aims. Simultaneously, U.S. military forces maintain the ability to better defend and protect the United States, its people, and interests in the homeland and abroad throughout a full spectrum of operations and contingencies.

The U.S. is conducting a global war on terrorism (GWOT). This national strategy is offensive, direct, and continuous.[474] U.S. action will initially disrupt, over time degrade, and ultimately destroy terrorist organizations of global reach.[475]

---

[473] Field Manual [U.S. Army] 7-100, Opposing Force Doctrinal Framework and Strategy, Headquarters, Department of the Army, iv to x, xvi (Washington, D.C., 2003). See discussion of DOD operating environment and Army description on contemporary operational environment (COE) "constants" and "critical variables."
[474] The White House, *The National Security Strategy of the United Sates of America*, Section III and IX, 17 September 2002; available at http://www.whitehouse.gov/nsc/nss.html; Internet; accessed 30 April 2004.
[475] The White House, *National Strategy for Combating Terrorism*, 2, February 2003; available at http://www.state.gov/s/ct/rls/rm/2003/17798.htm; Internet; accessed 30 April 2004.

Targets of U.S. operations will include terrorist leaders; their command, control, and communications; material support; and their finances. The war on terrorism will be fought on many fronts against a particularly elusive enemy over an extended period of time.

Case Study Purpose

Know your enemy. This can be a two-edged sword of situational awareness and understanding. By discerning threats and capabilities with documented terrorist incidents, U.S. military leaders will develop better situational awareness of forces and vectors of terrorism.

This understanding enables adaptive, proactive, deliberate processes of military risk management, force protection, mission orders conduct, and leader decisionmaking.

Case Study Elements. Case study method is a process of shared responsibility and disciplined exploration. In this terrorism handbook, case study organization comprises three main elements of (1) a case study abstract; (2) a main body comprising an introduction, learning objectives, situational overview, focus areas, case study discussion questions, and a brief case assessment; and (3) a listing of selected open-source references. The references are a prompt to seek additional resources through multi-media research and study.

Case study is an effective adult learning method that "…provides an opportunity to gain confidence in one's own judgment, but also a degree of humility as well. It also provides a most invaluable opportunity to learn how far one can go by rigorous logical analyses of one of the other dimensions of the problem and the extent to which judgment comes into play when many factors which have no common denominator must be weighed."[476]

This process guides, but does not dictate, a learning outcome. Using the case method, every iteration "…provides opportunity for new intellectual adventure, for risk taking, for new learning. One may have taught [studied] the case before, but last year's notes have limited current value. With a new group of students [leaders], the unfolding dynamic of a unique section, and different time circumstances, familiar material is revitalized."[477]

Abstract. A brief statement summarizes the case study and its significant observations on foreign or domestic terrorism.

Introduction. A preface presents the principal contents and purpose of the case study. Providing background information, the introduction provides context to the incident and enhances an appreciation of the sequence of events and act of terrorism.

---

[476] Louis B. Barnes, C. Roland Christensen, and Abby J. Hansen. *Teaching and the Case Method*. (Boston: Harvard Business School Press, 1994), 41.
[477] Ibid., 42.

Case Methodology

The case study presents, analyzes, and assesses salient aspects of a terrorism act. This method evolves from an overarching study of selected terrorism characteristics, specified learning objectives, case questions which focus analysis, and a summarized assessment of the analysis for discussion. Research data comes from unclassified sources and is available from common open-source portals.

Learning Objectives. The group of intended outcomes from the case study enables focused study, discussion, and analysis of a specific terrorist incident.

Case Questions. Issues, stated as open-ended questions, propose primary study topics. These queries explore relationships of terrorist tactics, techniques and procedures (TTP), and how terrorist capabilities were implemented to achieve a terrorist objective.

Assessment. Cogent statements summarize deliberate analyses of causal factors or linked relationships in a specified act of terrorism, and present informed conclusions to optimize planning and actions against terrorism capabilities.

Resources

Several references provide a credible baseline in case study use, and promote understanding key aspects of terrorism planning and operations in the contemporary operating environment:

Barnes, Louis B., C. Roland Christensen, and Abby J. Hansen. *Teaching and the Case Method*. Boston: Harvard Business School Press, 1994.

Field Manual [U.S. Army] 7-100. *Opposing Force Doctrinal Framework and Strategy* (Washington, D.C.: Headquarters, Department of the Army, 2003).

Tellis, W. Introduction to case study [68 paragraphs]. *The Qualitative Report* [On-line serial], *3*(2), July 1997. Available from: http://www.nova.edu/ssss/QR/QR3-2/tellisl.html; Internet; accessed 12 February 2004. [Do www.google.com search for "Tellis."]

Yin, R., *Case Study Research: Design and Methods* (2nd ed.) (Beverly Hills, CA: Sage Publishing, 1994).

Case Studies in this Appendix

- Murrah Federal Building, Oklahoma City, Oklahoma, USA (1995)

- Khobar Towers, Dhahran, Saudi Arabia (1996)

- USS *Cole*, Aden Harbor, Yemen (2000)

Page Intentionally Blank

Case Study – Murrah Federal Building (1995)

Abstract: Murrah Federal Building

The truck bombing of the Murrah Federal Building in Oklahoma City, Oklahoma, on April 19, 1995, signaled a horrific escalation of domestic terrorism conducted in the United States homeland.

> **"This is the place, after all, where terrorists don't venture. The Heartland. Wednesday [April 19] changed everything."**[478]

<div align="center">

The Daily Oklahoman
April 20, 1995

</div>

This act of domestic terrorism highlights the importance of accurate and timely intelligence on potential terrorist activities and capabilities, while preserving the individual rights and liberties of our democracy. The shock of this devastating attack was much more than physical damage. The psychological impact, both near-term and long-term, propelled each United States citizen into a stark recognition that domestic terrorism truly exists within the nation's borders. This example of terrorism in a contemporary operational environment illustrates an emergent terrorist trend of mass casualty or mass destruction effects as a terrorist objective.

Figure J-2. *Below,* **FBI Forensic Sketch and Photograph of Timothy McVeigh**

McVeigh was convicted for the bombing of the Murrah Federal Building.

He was executed June 11, 2001.

[479]

Figure J-1. *Above,* **Overhead View of Murrah Building Damage**[480]

---

[478] Department of Justice, Office of Justice programs, Office for Victims of Crime, *Responding to Terrorism Victims* (October 2000), ix, by Kathryn M. Turman, Director; available at http://www.ojp.usdoj.gov/ovc//publications/infores/respterrorism/welcome.html; Internet; accessed 11 March 2004.

[479] Photo Image; available at http://www.fbi.gov/hq/lab/org/ipgu.htm; Internet; accessed 11 March 2004.

This incident was, ultimately, the wanton act of one person. This case study presents an unclassified summary of a calculated strategy and tactics for a specific terrorist act based on U.S. findings in the criminal prosecution of Timothy McVeigh and his co-conspirator.

A primary underlying aim of terrorism is a demoralizing psychological effect on a target population and leaders to erode resolve and enhance other terrorist objectives. This was clearly McVeigh's goal when he selected a government target in the "heart of America."

Introduction

The U.S. Department of Justice provided a concise summary on physical effects and casualties of the bombing. The blast at the Alfred P. Murrah Federal Building killed 167 men, women, and children and injured 853 others. A volunteer nurse became the 168th fatality when she was struck by falling debris during the emergency response. The explosion devastated downtown Oklahoma City. The blast reduced the north face of the Murrah Building to rubble, and caused extensive damage to each of the nine floors as they collapsed into the center. When the dust cleared, one-third of the building lay in ruins. The force of the blast damaged 324 surrounding buildings, overturned automobiles, started fires, shattered windows, and blew out doors in a 50-block area. News reports indicated that the blast was felt 55 miles from the site and registered 6.0 on the Richter scale.

Nineteen children died and thirty children were orphaned in the Murrah Building's collapse. More than 400 individuals were left homeless in the area. When the bomb detonated, about 600 Federal and contract employees and about 250 visitors were in the building. Additionally, 7000 people lost their workplace. Approximately 16,000 people were in the downtown area in Oklahoma City at the time of the explosion. Beyond the physical devastation and death or injury to initial victims, the terrorist attack caused significant psychological and emotional impacts on a much larger population.[481]

Learning Objectives

Learning objectives focus on analyzing case study information in order to synthesize and evaluate the insight of reflective experiences, discern patterns of terrorist method and means, and determine likely trends in future terrorist activities. Comparing and contrasting conditions, circumstances, and options available to the terrorist will enhance the ability to recognize vulnerabilities and identify threats.

The objectives for this case study are:

- Describe intelligence indicators that would have alerted law enforcement to the threat.

- Understand the motivation of Timothy McVeigh for choosing the Murrah Building as a terrorist target of high value, as well as his selection of a symbolic date for the attack.

---

[480] Photo Image; available at http://www.hq.usace.army.mil/cepa/pubs/aug01/murrah.jpg; Internet; accessed 11 March 2004.

[481] Turman, Department of Justice, *Responding to Terrorism Victims,* 1.

- Recognize the domestic terrorist threat to U.S. forces and citizenry in the United States homeland.

- Explain the terrorist organizational structure and tactics, techniques, and procedures (TTP) used for the Murrah Building bombing.

- Deduce a trend for terrorist acts with the objective of an increased combination for mass casualties and mass destruction.

"Terrorism has now exploded into middle America."[482]

> Louis J. Freeh
> Director
> Federal Bureau of Investigation

Case Study - Murrah Federal Building (1995)

Overview

At 9:02 the morning of April 19, 1995 a catastrophic explosion ripped the air in downtown Oklahoma City. A truck bomb instantaneously demolished the entire front of the Alfred P. Murrah Federal Building. Tons of crashing concrete and metal disrupted governmental functions and destroyed scores of lives. These innocent Americans included clerks, secretaries, law enforcement officers, credit union employees, citizens applying for Social Security, and children.[483]

The Alfred P. Murrah Federal Building was used by various agencies of the United States, including the Agriculture Department, Department of the Army, Defense Department, Federal Highway Administration, General Accounting Office, General Services Administration, Social Security Administration, Housing and Urban Development, Drug Enforcement Administration, Labor Department, Marine Corps, Small Business Administration, Transportation Department, United States Secret Service, Bureau of Alcohol, Tobacco, and Firearms and Veterans Administration.[484]

---

[482] Louis J. Freeh, Director, Federal Bureau of Investigation; Congress, House of Representatives; Committee on the Judiciary Subcommittee on Crime; Opening Statement Before the Committee on the Judiciary Subcommittee on Crime, 104th Congress, 3 May 1995, 2; available from http://www.lectlaw.com/files/cur13.htm; Internet; accessed 5 March 2004.

[483] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. United States of America, Plaintiff, vs. Timothy James McVeigh, Defendant. The McVeigh Trial's April 24, 1997 Opening Statement by the [U.S.] Government; 3; available from http://www.lectlaw.com/bomb.html; Internet; accessed 5 March 2004.

[484] U.S. District Court, Western District of Oklahoma. Case No. M-95-105-H, United States of America, Plaintiff, vs. Terry Lynn Nichols, Defendant. "Terry Nichols Criminal Complaint," Affidavit; 1995, 2; available from http://www.lectlaw.com/files/cur18.htm; Internet; accessed 16 February 2004.

The primary preparation for this criminal act began on or about September 13, 1994 and culminated on April 19, 1995 in the bombing of the Alfred P. Murrah Federal Building in downtown Oklahoma City, Oklahoma.[485]

A chronology of terrorist activities displays an obsessive hate for the U.S. government, and a deliberate methodology for planning, preparing, and executing this terrorist attack.

Background

Surveying the lifestyle of Timothy McVeigh in the years prior to the bombing, he experienced mixed success at a series of minor jobs. He worked at a fast food restaurant in the fall of 1986 until the spring of 1987. Then he switched jobs and went to work as an armored car driver for a commercial security company in Buffalo, New York from the spring of 1987 to the spring of 1988.

McVeigh joined the U.S. Army in May, 1988 and remained in the Army until late 1991. He was a successful gunner on a mechanized infantry vehicle during the Gulf War and was decorated with several Army awards for actions in combat and commendable service. [486] Yet, McVeigh's dislike for the Federal government was revealing itself in this same period. Some of his discussions with acquaintances related to reading a book and the exploits of a group of well-armed men and women who called themselves "patriots" that sought to overthrow the Federal government by use of force and violence. In one book, a group makes a fertilizer bomb in the back of a truck and detonates it in front of a Federal building in downtown Washington, D.C. during business hours that kills hundreds of people.[487]

As a guard for a commercial security company, he distributed white supremacist pamphlets and a book to co-workers on how to avoid paying taxes, and commented that it would be easy to steal firearms from a military base.[488] From March 1992 to early 1993, McVeigh worked at another commercial security service. He visited his friends Mike and Lori Fortier who lived in Arizona. McVeigh worked at a hardware store in Arizona, and also worked as a security guard. Eventually, he started buying and selling books, as well as survivalist items at numerous gun shows throughout the United States.

McVeigh was fixated on personal rights and individual freedom. He studied history, the U.S. Constitution, and the amendments to the Constitution. He carried them on his person, he carried them in his car, and he carried them in his briefcase. He stacked them in his house, and he displayed them on tables at gun shows.

---

[485] U.S. District Court, District of Colorado. Criminal Action No. 95-CR-110 United States of America, Plaintiff, vs. Timothy James McVeigh and Terry Lynn Nichols, Defendants. "8/95 Grand Jury Indictment of McVeigh and Nichols," Indictment Count One (Conspiracy to Use a Weapon of Mass Destruction); 1995, 1; available from http://www.lectlaw.com/files/cas44.htm; Internet; accessed 2 February 2004.

[486] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. United States of America, Plaintiff, vs. Timothy James McVeigh, Defendant. The McVeigh Trial's April 24, 1997 Opening Statement by the Defense; 5 and 6; available from http://www.lectlaw.com/bomb.html; Internet; accessed 5 March 2004.

[487] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the [U.S.] Government; 6 and 7; available from http://www.lectlaw.com/bomb.html; Internet; accessed 5 March 2004.

[488] Lou Michel and Dan Herbeck, *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing* (New York: Harper Collins Publishers Inc., 2001), 113.

He also wrote letters to newspapers with his viewpoint on personal rights and freedoms. He voted as a U.S. citizen. His politics were openly expressed and known to everyone that spent time with him.[489] In touring gun shows throughout the United States, he eventually visited forty of fifty states. As he sold books and survival items at gun shows, he often met people with similar concern about Constitutional rights and the perceived Federal government's zeal in gun control.[490]

McVeigh viewed the Federal raid at Ruby Ridge in 1992 as another incident of government attack on individual freedoms. Incidents between U.S. citizens and Federal agents such as at Ruby Ridge [1992] and Waco [1993] greatly concerned McVeigh. Citizens could have distinctly different beliefs and commitment to how individual rights[491] and obedience to and enforcement of law[492] are expressed in the United States. According to McVeigh's defense attorney at his trial after the Murrah Building bombing, McVeigh was angry about Ruby Ridge. He believed that the ATF had entrapped Randy Weaver into committing a crime so that they could then pressure Weaver into being an informant for the ATF [Alcohol, Tobacco, and Firearms] in a community in northern Idaho. McVeigh believed that the Federal government had acted very unjustly in the incident that resulted in the death of a Federal agent, the killing of Randy Weaver's wife, and the killing of a ten-year-old boy as he was running towards the Weaver's house. A court jury acquitting Randy Weaver of murder in the Ruby Ridge incident further convinced McVeigh of the correctness of his belief.

McVeigh also strongly opposed to the Brady Bill and gun control, so he wrote angry letters and talked about freedom and citizen's constitutional rights. In McVeigh's mind, the Brady Bill was just the first step to effectively repeal the U.S. Constitution's Second Amendment by taking away from people their right to own guns and to protect themselves against abuses of the Federal government.[493]

In addition to his concerns on the Ruby Ridge incident and the Brady Bill, McVeigh became obsessed with the outcome of the Waco, Texas incident between a religious group known as the Branch Davidians and Federal agents from the Bureau of Alcohol, Tobacco, and Firearms. An attempt to serve a search warrant for illegal weapons resulted in a gunfire exchange that resulted in several deaths and a group of Branch Davidians barricading themselves inside their ranch compound. He traveled to the Waco site and distributed anti-governmental literature. On April 19th, 1993, the United States experienced another tragedy when the siege of the Branch Davidian compound resulted in several deaths and destruction of the compound. McVeigh believed that the Federal government executed 76 people at Waco, including 30 women and 25 children. He believed that the Federal law enforcement at Waco deployed in a military fashion against American citizens and children living as a religious group in a

---

[489] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the Defense, 8.

[490] Michel and Herbeck, *American Terrorist,* 121.

[491] *"Ruby Ridge Federal Siege, Bibliography"* [bibliography on-line]; available from http://users.skynet.be/terrroism/html/usa_ruby_ridge.htm; Internet; accessed 16 March 2004.

[492] *"Waco – Branch Davidian Files,"* available from http://www.paperlessarchives.com/waco.html; Internet; accessed 16 March 2004.

[493] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the Defense, 9.

compound, who had committed no crime.[494]   McVeigh visited Waco during the siege and went back after the compound's fire and final events of the siege.

As time passed, he became more outraged at the government. McVeigh told people that the U.S. Federal Government had intentionally murdered people at Waco, and described the incident as the government's declaration of war against the American people. He wrote letters declaring that the government had drawn "first blood" at Waco, and predicted there would be a violent revolution against the American government.

McVeigh's anger and hatred of the government kept growing, and in late summer 1994, he told friends that he was done distributing antigovernment propaganda and talking about the coming revolution. He said it was time to take action, and the action he wanted to take was something dramatic, something that would shake up America [United States]. McVeigh expected and hoped that his action would be the "first shot" in a violent, bloody revolution in this country. [495]

Planning and Preparation

The action he selected was a bombing, and the building he selected was the Murrah Federal Building in Oklahoma City. McVeigh had two reasons for bombing that particular building. First, he thought that the ATF agents, whom he blamed for the Waco tragedy, had their offices in that building. Second, McVeigh described the Murrah Federal Building as "an easy target."[496]

McVeigh selected the Murrah Building from a list of sites he developed as potential targets. He wanted his attack to target Federal law enforcement agencies and their employees. He recognized that many innocent people would be injured or killed. Primary targets included the Bureau of Alcohol, Tobacco, and Firearms; Federal Bureau of Investigation; and Drug Enforcement Administration. Besides the Oklahoma City site, McVeigh considered locations in Arkansas, Arizona, Missouri, and Texas. Another possible site may have included Washington, D.C. McVeigh considered targeting specific Federal individuals or their family members, but decided that a bombing would cause more notoriety.[497]

The Murrah Building was conveniently located just south of Kansas where McVeigh resided. Its close proximity to an interstate highway (Interstate 35) assured easy access to and egress from the bombing target.   The building design allowed for easy delivery or pickup of packages and people due to indented curbing in front of the building, which allowed vehicles to park directly in front of the building. You could drive a truck directly up to the front of the building.[498] McVeigh assessed the damage that would occur based on the extensive amount of

---

[494] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the Defense; 8.

[495] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the [U.S.] Government, 7.
[496] Ibid., 8.
[497] Michel and Herbeck, *American Terrorist,*167 and 168.
[498] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the [U.S.] Government, 9.

glass windows in the Murrah Building and considered the probable collateral damage to surrounding structures. He recognized that the open parking lot space across the street from the building may dissipate some concussion from the explosion, but would allow good photograph coverage of a stark, horrifying image. Killing a large number of Federal employees was part of his plan to ensure major media attention.[499]

McVeigh conducted detailed personal reconnaissance of his target and routes of approach and routes of escape.[500]   McVeigh memorized his sequence of actions for this bombing, rehearsed his route, and prepared mentally for contingencies such as flat tires or meeting with police.[501]

McVeigh practiced bomb construction and observed bomb effects on a small scale by using a plastic jug and detonating the explosive-packed device at a desert location near a friend's home.[502] The bomb concept McVeigh was planning consisted of more than 5000 pounds of ammonium nitrate fertilizer mixed with about 1200 pounds of liquid nitromethane, 350 pounds of Tovex explosive, and the miscellaneous weight of sixteen 55-gallon drums, for a combined weight of about 7000 pounds.[503] The truck bomb was relatively inexpensive to construct. A truck rental would be about $250. Fertilizer would cost about $500. The nitromethane cost about $3000. A used car for his escape vehicle would cost about $250. His estimate was a bomb project costing approximately $5000.[504]

McVeigh and Nichols obtained 4,000 pounds − two tons − of ammonium nitrate fertilizer. They bought it at a farm supply store in central Kansas where Nichols was living at the time and where McVeigh visited him. This was in the fall of 1994, at least six months before the bombing; giving an indication of the deliberate planning that went into process and premeditation.[505] To get some of the other chemicals they needed for the bomb, McVeigh and Nichols used a commercial phone book and simply called dozens of companies and individuals in search of ingredients.[506]

McVeigh and Nichols got the detonators for the bomb by stealing them. Near Marion, Kansas, they broke into several storage lockers for explosives at a rock quarry, and stole hundreds of blasting caps and sausage-shaped explosives known as Tovex.[507] They rented storage lockers in the central Kansas area near Nichols home and in Arizona to store supplies and stolen items, using phony names to preclude easy tracing of their real identities.[508]

During this period when McVeigh and Nichols were acquiring the components for the bomb, McVeigh periodically drove to Arizona and visited two of his friends, Michael and Lori Fortier. He had met Michael in the Army. They had shared similar antigovernment ideas,

---

[499] Michel and Herbeck, *American Terrorist,*168 and 169.
[500] Ibid., 230.
[501] Ibid., 214 and 215.
[502] Ibid., 165.
[503] Ibid., 164.
[504] Ibid., 176 and 207.
[505] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the [U.S.] Government, 9.
[506] Ibid., 10.
[507] Ibid., 13.
[508] Ibid., 14.

and McVeigh had come to trust Michael and Michael's wife, Lori. In the fall of 1994, he confided his plan to both of them. Sitting in their living room in Kingman, Arizona, McVeigh drew a diagram of the bomb that he intended to build. He outlined the box of the truck and drew circles for the barrels inside the truck. He described how the barrels of fertilizer and fuel oil would be positioned in the truck to cause maximum damage. McVeigh demonstrated his design to Lori Fortier by taking soup cans from her cupboard and placing them on the floor. The layout displayed the shape of the bomb inside the box of the truck that he described as a shape charge. He explained that by putting the barrels of explosives in a particular shape, he would increase the blast effects in a particular direction.[509]

In addition to what McVeigh told Fortier about his bombing plans, he took Fortier to Oklahoma City and showed him the building months before the bombing. McVeigh told Fortier during the trip that Nichols would help McVeigh mix the bomb and would help McVeigh get away after the bombing. When McVeigh and Fortier were in downtown Oklahoma City, they drove around the Murrah Building. McVeigh showed Fortier the alley where he planned on parking his car. He explained to Fortier that he would park there because he wanted to have a tall building between himself and the blast.[510]

McVeigh also told Fortier about how he and Nichols planned to raise money to finance their illegal activities. They were going to do it by robbing a man who was a gun dealer that McVeigh knew from Arkansas. McVeigh had previously observed the man's home in a remote area of Arkansas.[511] Since the man knew McVeigh, Nichols was going to do the actual robbery. The stolen weapons and property were eventually sold to finance the bombing plot.

Table J-1. Conspiracy Timeline for Murrah Building Bombing ("On or About Dates" [512])	
Chronology	**Event**
September 22, 1994	McVEIGH rented a storage unit in the name of "Shawn Rivers" Herington, Kansas.
September 30, 1994	McVEIGH and NICHOLS purchased forty fifty-pound bags of ammonium nitrate in McPherson, Kansas under name of "Mike Havens."
Late September 1994	McVEIGH made telephone calls in an attempt to obtain detonation cord and racing fuel.
October 1, 1994	McVEIGH and NICHOLS stole explosives from a storage locker (commonly referred to as a magazine) in Marion, Kansas.

---

[509] Ibid., 15.

[510] Ibid., 32.

[511] Ibid.

[512] U.S. District Court, District of Colorado. Criminal Action No. 95-CR-110 United States of America, Plaintiff, vs. Timothy James McVeigh and Terry Lynn Nichols, Defendants. "8/95 Grand Jury Indictment of McVeigh and Nichols," Indictment Count One (Conspiracy to Use a Weapon of Mass Destruction); 1995, 2 to 4; available from http://www.lectlaw.com/files/cas44.htm; Internet; accessed 2 February 2004.

October 3, 1994	McVEIGH and NICHOLS transported the stolen explosives to Kingman, Arizona.
October 4, 1994	McVEIGH rented a storage unit in Kingman, Arizona for the stolen explosives.
October 16, 1994	NICHOLS registered at a motel in Salina, Kansas under the name "Terry Havens."
October 17, 1994	NICHOLS rented storage unit No. 40 in Council Grove, Kansas in the name "Joe Kyle."
About October 18, 1994	McVEIGH and NICHOLS purchased forty fifty-pound bags of ammonium nitrate in McPherson, Kansas under the name "Mike Havens."
October 1994	McVEIGH and NICHOLS planned a robbery of a firearms dealer in Arkansas as a means to obtain moneys to help finance their planned act of violence.
November 5, 1994	McVEIGH planned and NICHOLS robbed, at gunpoint, a firearms dealer in Arkansas of firearms, ammunition, coins, United States currency, precious metals and other property.
November 7, 1994	NICHOLS rented storage unit No. 37 in Council Grove, KS in the name "Ted Parker" and concealed property stolen in the Arkansas robbery.
November 16, 1994	NICHOLS rented a storage unit in Las Vegas, Nevada and stored items.
November 21, 1994	NICHOLS prepared a letter to McVEIGH, to be delivered only in the event of NICHOLS' death, in which he advised McVEIGH, among other matters, that storage unit No. 37 in Council Grove, Kansas had been rented in the name "Parker" and instructed McVEIGH to clear out the contents or extend the lease on No. 37 by February 1, 1995. NICHOLS further instructed McVEIGH to "liquidate" storage unit No. 40.
December 16, 1994	McVEIGH, while en route to Kansas to take possession of firearms stolen in the Arkansas robbery, drove with Michael FORTIER to the Alfred P. Murrah Federal Building and identified the building as the target.
Early 1995	McVEIGH, NICHOLS, and FORTIER obtained currency from sale of firearms stolen in the Arkansas robbery.
February 9, 1995,	NICHOLS paid for the continued use of storage unit No. 40 at Council Grove, Kansas in the name of "Joe Kyle."
March 1995	McVEIGH obtained a driver's license in the name of "Robert Kling" bearing a date of birth of April 19, 1972.
April 14, 1995	McVEIGH purchased a 1977 Mercury Marquis in Junction City, KS.
April 14, 1995	McVEIGH called the NICHOLS residence in Herington, Kansas from Junction City, KS.
April 14, 1995,	McVEIGH called a business in Junction City using the name "Bob Kling" to inquire about renting a truck capable of carrying 5,000 pounds of cargo.
April 14, 1995	McVEIGH rented a room at a motel in Junction City, KS.

April 15, 1995	McVEIGH placed a deposit for a rental truck in the name "Robert Kling."
April 17, 1995	McVEIGH took possession of a 20-foot rental truck in Junction City, KS.
April 18, 1995	McVEIGH and NICHOLS, at Geary Lake State Park in Kansas, constructed an explosive truck bomb with barrels filled with a mixture of ammonium nitrate, fuel and other explosives placed in the cargo compartment of the rental truck.
April 19, 1995	McVEIGH caused the truck bomb to explode by lighting fuses connected to the explosive device in the truck.
April 19, 1995	McVEIGH parked the truck bomb directly outside the Alfred P. Murrah Federal Building in downtown Oklahoma City, Oklahoma, during regular business and day-care hours.
April 19, 1995 9:02	**Truck bomb detonates next to Alfred P. Murrah Federal Building.**

McVeigh learned some of his bomb making knowledge from pamphlets or books easily available on the open market. He learned how to mix different explosive ingredients, how to set up the bomb; and details such as how to drill a hole between the cargo box and the cab of the truck so that he could light the fuse from where he would be sitting as he drove the truck bomb.[513]

By the end of October 1994, McVeigh had most of the ingredients he needed to build the bomb. He was determined to take action when he thought it would have maximum impact. The anniversary of the tragedy at Waco would provide that kind of maximum impact. He thought that others in the U.S. were as angered at Waco as he was and that he could achieve tremendous impact – shake up the nation – by delaying his violent terrorist action until the April 19th anniversary of the Waco incident.[514]

"Something big is about to happen."[515]

Timothy McVeigh
Letter to McVeigh's sister

McVeigh had been regularly corresponding with his sister, Jennifer. In the fall of 1994, he visited her and created a file in her computer. He marked the file "ATF read," as though he wanted the ATF to discover this file and read it after his dramatic action. One chilling declaration stated, "All you tyrannical [profanity] will swing in the wind one day for your treasonous actions against the Constitution and the United States." The file entry concluded with these words: "Die, you spineless cowardice [profanity]."

---

[513] Ibid., 25.
[514] Ibid., 15.
[515] Ibid., 16.

On occasion, McVeigh used pre-paid debit cards or public pay telephones to avoid the possibility of calls being traced to him. For instance, on April 14th McVeigh called Terry Nichols, who was living at that time in nearby Herington, Kansas. McVeigh also called a company to reserve a rental truck. Both calls were made on a debit card in an attempt to preclude any trace of who actually called.

Later that day, McVeigh registered with his own name at a small motel in Junction City, Kansas. He resided at the motel through that weekend up until April 18th, Tuesday, the day before the bombing.[516]

To hide his true identity, McVeigh used a phony driver's license to rent a truck. He had obtained a blank driver's license form through an advertisement in a commercial magazine that sells fake identification kits. He selected the name Robert Kling. As McVeigh noted to Lori Fortier, he liked that name because it reminded him of the "Klingon" warrior characters on a popular television show "Star Trek."[517]

Located about four miles from the motel, McVeigh arrived at a truck rental agency. The truck rental company attendant remembered a young man with a military demeanor who introduced himself as Robert Kling. Instead of simply making a cash deposit to reserve the truck in the name Kling, this man [McVeigh] wanted to pay for the truck in full. Kling [McVeigh] counted out several hundred dollars in cash and gave it to the attendant. After some administering of forms, Kling [McVeigh] departed the truck rental company, saying he would return to pick up the truck.[518]

As a sidenote, April 23d is McVeigh's real birthday. However, the birthday he gave Kling on the fake driver's license used to "prove" his identify was a special day -- April 19th -- the anniversary of the Davidian incident at Waco, and the date that McVeigh selected for the bombing in Oklahoma City.[519] McVeigh wanted to avenge the deaths that occurred at Waco. He also knew that April 19th in 1775 is considered by some people as the beginning of the American Revolution[520] and in his own mind, would be symbolic of defiance against what he believed to be an oppressive government.

On the morning of April 18, 1995, an individual at the Geary State Fishing Lake, approximately six miles south of Junction City, Kansas, observed a yellow truck parked next to a pickup truck for several hours. The individual described the pickup truck in some detail and recalled there was something white, possibly a camper shell, on the back of the pickup truck.[521] Little did the observing individual know that two men (McVeigh and Nichols) were constructing a massive truck bomb that would devastate the Murrah Building the next day in Oklahoma City.

---

[516] Ibid., 19.

[517] Ibid., 17.

[518] Ibid., 19-21.

[519] Ibid., 24.

[520] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the [U.S.] Government, 9.

[521] U.S. District Court, Western District of Oklahoma. Case No. M-95-105-H, "Terry Nichols Criminal Complaint," 6.

The Attack

Sleeping in the rental truck that night at a gravel lot near a roadside motel in northern Oklahoma, McVeigh awoke early the morning of April 19th, 1995. As he entered downtown Oklahoma City, he placed earplugs in his ears and continued driving. He stopped briefly to light one of two fuses connected to the bomb. Shortly afterwards, he halted the truck for a stoplight and lit the second fuse. The Murrah Building and surrounding area, brimming with people, were about to become a macabre scene of devastation.

McVeigh positioned the truck at the delivery access point in front of the Murrah Building, got out of the truck and locked the vehicle. He walked casually on a route along sidewalks that he had previously reconnoitered. He wanted to be behind a building when the bomb detonated. As the roar of the explosion shattered the morning air, McVeigh was lifted a full inch off the ground by the blast and recalled his cheeks being buffeted by the concussion. He didn't look back. Within seconds, McVeigh was in his car and heading north out of the city.[522]

The Immediate Aftermath

After the bomb exploded, McVeigh calmly, at least outwardly, departed the bombing scene. McVeigh said he felt satisfaction of a mission accomplished. McVeigh had previously driven his car to Oklahoma City on Easter Sunday and prepositioned it near the Murrah Building as a means to depart the area after the bombing.[523] Within seconds of the detonation, McVeigh was driving his car north out of the city.[524]

About an hour after the bombing, an alert Highway Patrol trooper driving on Interstate 35 stopped a Mercury Marquis automobile because there was no car license plate on the back of the vehicle. He asked the driver (McVeigh) for his driver's license, and noticed a bulge under his clothing. McVeigh told the police officer that he had a loaded pistol and cooperated with the police officer as he was arrested. Yet, certain actions are puzzling about McVeigh. His post-trial reflections recount his thoughts when approached by the state trooper as McVeigh waited in his car by the side of the highway. McVeigh could have easily surprised and harmed the state trooper with a loaded pistol he was carrying on his person, but he chose not to do anything aggressive. At the time, the police officer made no connection with the bombing in Oklahoma City and McVeigh. He put McVeigh under arrest and drove to the county seat.[525]

On April 21, 1995, investigators learned that at approximately 10:20 a.m. on April 19, 1995, Timothy McVeigh had been arrested in Oklahoma on traffic and weapon offenses, and was incarcerated on those charges in Perry, Oklahoma. McVeigh's arrest occurred approximately

---

[522] Michel and Herbeck, *American Terrorist,* 220, 229-232.

[523] U.S. District Court, District of Colorado. Criminal Action No. 95-CR-110 United States of America, 20.

[524] Michel and Herbeck, *American Terrorist,* 232, 237.

[525] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the Defense, 42.

60-70 miles north of Oklahoma City, Oklahoma, approximately one hour and 20 minutes after the April 19, 1995 bomb explosion.[526]

Inside McVeigh's car, law enforcement agents later found a large sealed envelope. It contained writings, magazines, and photocopies from magazines and from newspapers that indicate McVeigh's motivation, and premeditation. Other documents that McVeigh had with him on this day of the bombing describe the value of killing innocent people for a cause. One excerpt – as highlighted by McVeigh – "The real value of our attacks today lies in the psychological impact, not in the immediate casualties." Another slip of paper that he had in that envelope in his car read, in part, "When the government fears the people, there is liberty." And hand-printed beneath those printed words, in McVeigh's handwriting, are the words, "Maybe now there will be liberty."[527]

Fortier

Fortier was culpable in the bombing. Although he did not join the conspiracy and he didn't participate in the bombing, he did have knowledge of McVeigh's plans. He neither reported it to anyone who could have stopped it, nor made any effort to prevent the criminal acts. Additionally, Fortier participated with McVeigh in transporting guns stolen from a gun dealer in Arkansas.[528]

Mr. Fortier agreed to enter a plea bargain, was found guilty by a jury trial, and sentenced to 12 years in prison and fined $200,000.[529]

Nichols

On April 21, 1995, at approximately 3:00 p.m., after hearing his name on the radio in connection with the Oklahoma City bombing, Terry Nichols voluntarily surrendered to the Department of Public Safety in Herington, Kansas. Herington authorities took no action and awaited the arrival of the FBI. Thereafter, a Special Agent of the FBI arrived and advised Nichols of his Miranda rights, which Nichols agreed to waive.[530]

Although Nichols did not participate in the actual bombing, he was instrumental in assisting McVeigh in planning and preparing for the bombing. He helped rent storage lockers, purchase ammonium nitrate fertilizer and place McVeigh's get-away car in Oklahoma City. In a Federal Court, Nichols was convicted of conspiracy, and found guilty of involuntary manslaughter in the death of eight Federal officers.[531]

---

[526] U.S. District Court, Western District of Oklahoma. Case No. M-95-105-H, "Terry Nichols Criminal Complaint," 3.

[527] U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. Opening Statement by the [U.S.] Government, 4 and 5.

[528] Ibid., 34.

[529] "Oklahoma Bombing Chronology," *Washington Post*, available from http://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/chron.htm; Internet; accessed 5 March 2004.

[530] U.S. District Court, Western District of Oklahoma, Case No. M-95-105-H, "Michael Fortier's Plea Agreement," 3.

[531] Richard A. Serrano, "Terry Nichols Sentenced to Life With No Hope of Parole," *Los Angeles Times*, available from http://www.-tech.mit.edu/V118/N27/nichols.27w.htm; Internet; accessed 16 February 2004.

After being found guilty in a Federal jury trial, Nichols was sentenced to life in prison without release for his role as the chief collaborator in the Oklahoma City bombing. In August 2004, Nichols was found guilty of murder on Oklahoma state charges. The District Judge ordered Nichols to serve life imprisonment without the possibility of parole. Nichols was spared the death penalty when the jury became deadlocked.**[532]**

McVeigh

McVeigh was convicted on all 11 counts of his Federal Indictment, including conspiracy to bomb the building and responsibility for the deaths of eight Federal law enforcement officers killed inside.[533] Timothy McVeigh was executed at a Federal prison in Terra Haute, Indiana on June 11, 2001.

Case Discussion Questions

Intelligence and Threat Warning?

What suspicious activities preceding the bombing attack might have indicated the tactical targeting of the Murrah building in an operational level U.S. intelligence estimate?

Why did McVeigh select the Murrah Federal Building for his terrorist attack?

Planning, Preparation, and Conduct?

How did the terrorist cell obtain the major components of the improvised explosive device – the bomb?

How did the terrorist and support cell structure itself, communicate, and operate during the phases of planning and execution of the Murrah Building bombing attack?

How did the terrorist rehearse for the Murrah Building bombing?

What does the proximity of distance of the Murrah Building to the point of bomb detonation indicate for force protection measures?

Physical Site Vulnerabilities and Risk Assessment?

What specific effects did the truck bomb detonation have on the structural integrity of the Murrah Building?

Given the same type of truck bomb and the scenario of a multi-level downtown office building, how could terrorists have increased mass casualty effects and devastation?

---

[532] "Terry Nichols Gets Life, No Parole," CNN.com LAW CENTER, 10 August 2004; available on http://www.cnn.com/2004/LAW/08/09/Nichols.sentence.ap/; Internet; accessed 25 August 2004.
[533] Department of State, U.S. Department of State International information Programs, "Timothy McVeigh Executed for Oklahoma City Bombing," 11 June 2001; available on http://usinfo.state.gov/topical/pol/terror/01061101.htm; Internet; accessed 16 February 2004.

Assessment

As the bombing in Oklahoma City makes clear, Americans – domestic terrorists - with dastardly aims and intentions such as McVeigh must be considered in any threats profile of the U.S. Homeland. Noted by the Director of the FBI, "We cannot protect our country, our way of life, our government and the democratic processes that ensure our freedoms and liberties if we fail to take seriously the threat of terrorism from all sources – foreign and domestic."[534]

> **"Terrorism is best prevented by acquiring, through legal and constitutional means, intelligence information relating to groups and individuals whose violent intentions threaten the public or our nation's interests."[535]**
>
> Louis J. Freeh
> Director
> Federal Bureau of Investigation

McVeigh was a U.S. citizen with personal beliefs that festered into a growing mistrust and eventual hatred of the U.S. government.[536]

Awaiting execution, McVeigh remarked, "I like the phrase 'shot heard 'round the world,' and I don't think there's any doubt the Oklahoma blast was heard around the world."[537]

A comprehensive FBI investigation determined that there was no larger conspiracy than McVeigh and Nichols in the Murrah Building bombing. Over 43,000 leads and over 7,000 people were eliminated from consideration in this official scrutiny. No involvement of a foreign government or militia organization materialized, even though numerous allegations arose in conspiracy theories.[538]

In a May 1995 statement by the Director of the FBI, Mr. Louis Freeh stated, "I do not want my remarks to be interpreted as advocating investigative activity against groups exercising their legitimate constitutional rights or targeting people who disagree with our government. The FBI is entirely comfortable with the Constitution, due process rights, Congressional oversight, legal process, and the American jury system. They each protect the American people and the FBI…The FBI cannot and should not, however, tolerate and ignore any individuals or groups which advocate violence – which would kill innocent Americans, which

---

[534] Louis J. Freech, Director, Federal Bureau of Investigation; Opening Statement Before the Committee on the Judiciary Subcommittee on Crime, 3 May 1995, 2.
[535] Louis J. Freech, Director, Federal Bureau of Investigation; Congress, House of Representatives; Committee on the Judiciary Subcommittee on Crime; Opening Statement Before the Committee on the Judiciary Subcommittee on Crime, 104th Congress, 3 May 1995, 3; available from http://www.lectlaw.com/files/cur13.htm; Internet; accessed 5 March 2004.
[536] Michel and Herbeck, *American Terrorist,* 108.
[537] Ibid., 382.
[538] Ibid., 366.

would kill "America's Kids." They are not just enemies of the United States, they are enemies of mankind."[539]

Resources

Freeh, Louis J. Director, Federal Bureau of Investigation. U.S. Congress. House of Representatives. Committee on the Judiciary Subcommittee on Crime. Opening Statement by Louis J. Freeh, Director, Federal Bureau of Investigation Before the Committee on the Judiciary Subcommittee on Crime. 104th Congress, 3 May 1995. Available from http://www.lectlaw.com/files/cur13.htm; Internet; Accessed 5 March 2004.

Gorin, Stuart. "Timothy McVeigh Executed for Oklahoma City Bombing." Washington File Staff Writer; U.S. Department of State International Information Programs. 11 June 2001. Available from http://usinfo.state.gov/topical/pol/terrro/01061101.htm; Internet; Accessed 16 February 2004.

Michel, Lou and Dan Herbeck. *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing.* New York: Harper Collins Publishers Inc., 2001.

Serrano, Richard A. "Terry Nichols Sentenced to Life With No Hope of Parole." *Los Angeles Times*, 5 June 1998. Available from http://www.-tech.mit.edu/V118/N27/nichols.27w.htm; Internet; Accessed 16 February 2004.

"Oklahoma Bombing Chronology." *Washington Post.* Available from http://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/chron.htm; Internet; Accessed 5 March 2004.

"Ruby Ridge Federal Siege, Bibliography." [Bibliography on-line]. Available from http://users.skynet.be/terrroism/html/usa_ruby_ridge.htm; Internet; Accessed 16 March 2004.

U.S. Department of Justice. Office of Justice Programs. Office for Victims of Crime. *Responding to Terrorism Victims* (October 2000), by Kathryn M. Turman, Director, Available at http://www.ojp.usdoj.gov/ovc//publications/infores/respterrorism/welcome.html; Internet; Accessed 11 March 2004.

U.S. District Court, Western District of Oklahoma. Case No. M-95-105-H. United States of America. Plaintiff, vs. Terry Lynn Nichols, Defendant. "Terry Nichols Criminal Complaint," Affidavit. 9 May 1995, 2. Available from http://www.lectlaw.com/files/cur18.htm; Internet; Accessed 16 February 2004.

U.S. District Court. Western District of Oklahoma. Case No. M-95-105-H. United States of America. Plaintiff, vs. Michael J. Fortier, Defendant. "Michael Fortier's Plea Agreement," Affidavit. 10 August 1995, 2. Available from http://www.lectlaw.com/files/cas37.htm.; Internet; Accessed 16 February 2004.

U.S. District Court, District of Colorado. Criminal Action No. 95-CR-110. United States of America, Plaintiff, vs. Timothy James McVeigh and Terry Lynn Nichols, Defendants. "8/95 Grand Jury Indictment of McVeigh and Nichols." Indictment Count One (Conspiracy to Use a Weapon of Mass Destruction). 1995, 1. Available from http://www.lectlaw.com/files/cas44.htm; Internet; Accessed 2 February 2004.

U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. United States of America, Plaintiff, vs. Timothy James McVeigh, Defendant. The McVeigh Trial's April 24, 1997 Opening Statement by the [U.S.] Government. Available from http://www.lectlaw.com/bomb.html; Internet; Accessed 5 March 2004.

U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. United States of America, Plaintiff, vs. Timothy James McVeigh, Defendant. The McVeigh Trial's April 24, 1997 Opening Statement by the [U.S.] Government. Available from http://www.lectlaw.com/bomb.html; Internet; Accessed 5 March 2004.

"Waco – Branch Davidian Files." Available from http://www.paperlessarchives.com/waco.html; Internet; Accessed 16 March 2004.

---

[539] Louis J. Freech, Director, Federal Bureau of Investigation; Opening Statement Before the Committee on the Judiciary Subcommittee on Crime, 3 May 1995, 4.

Case Study – Khobar Towers Bombing (1996)

Abstract: Khobar Towers

The terrorist attack on Khobar Towers in 1996 highlights the importance of accurate and timely intelligence on terrorist activities and capabilities, the structure of a terrorist organization in action, and an emergent trend of mass casualty or mass destruction effects as a terrorist objective. This case study presents an unclassified summary of U.S. findings of intelligence shortfalls, force protection vulnerabilities, host nation operational sensitivities, and the calculated strategy and tactic of a specific terrorist act. In this case, a state sponsor assisted a surrogate group in order to influence U.S. policy in the Middle East.

Figure J-3. *Above,* **Bomb Crater from VBIED**

(*Source:* U.S. House National Security Committee, Staff Report, *The Khobar Towers Bombing Incident* (1996).)

Figure J-4. *Right,* **The Front View of Building 131 at Khobar Towers After the Blast**

(*Source:* U.S. House National Security Committee, Staff Report, *The Khobar Towers Bombing Incident* (1996).)

Introduction

The terrorist bombing of the Khobar Towers complex in Dhahran, Saudi Arabia on June 25, 1996 exposed more than the physical vulnerability of Americans serving abroad. The attack exposed shortcomings of the U.S. intelligence apparatus that left Americans unprepared for the specific threat that confronted them. U.S. military organizations encountered significant internal problems of continuity and cohesion with the host nation while deployed for their mission. Risk increased for U.S. military members deployed on contingency operations where political and cultural sensitivities of the host country were significant factors.[540] A chronology of terrorist group activities in this case demonstrates a dedicated motivation and deliberate planning and execution cycle that applied phases of reconnaissance and surveillance, specific target selection and refined surveillance, staging and rehearsal, attack, and escape.

> **"Terrorism is a tool of states, a vehicle of expression for organizations and even a way of life for individuals. We can expect the terrorists to continue to seek out vulnerabilities and attack. Terrorists normally prey on the weak, but even militaries have vulnerabilities and present targets with high publicity value."[541]**

> Secretary of Defense
> United States of America
> 1996

Learning Objectives

Learning objectives focus on analyzing case study information in order to synthesize and evaluate the insight of reflective experiences, discern patterns of terrorist method and means, and determine likely trends in future terrorist activities. Comparing and contrasting conditions, circumstances, and asymmetric options available to the terrorist will enhance judgment to recognize vulnerabilities, identify threats, and minimize the ability of terrorism to impact on accomplishing a friendly force mission.

The objectives for this case study are:

- Describe intelligence indicators that might have created a more effective tactical estimate of terrorist intention and capability in the Khobar Towers bombing.

- Understand the motivation of Saudi Hizballah and their state sponsor (Iran) associated support groups for choosing Khobar Towers as a terrorist target of high value.

---

[540] House National Security Committee, *Report on the Bombing of Khobar Towers* (14 August 1996), by Chairman Floyd D. Spence and Report, U.S. House National Security Committee, Executive Summary; available from http://www.fas.org/irp/threat/saudi.pdf; Internet; accessed 10 February 2004.

[541] Department of Defense. Report to the President. *The Protection of U.S. Forces Deployed Abroad* (15 September 1996) by Secretary of Defense William J. Perry, 14; available from http://www.fas.org/irp/threat/downing/report_f.html; Internet; accessed 18 February 2004.

- Recognize force protection vulnerabilities at Khobar Towers that terrorists optimized in the bombing attack.

- Explain the terrorist organizational structure and tactics, techniques, and procedures (TTP) used for the Khobar Towers bombing.

- Deduce a trend for terrorist acts with the objective of an increased combination for mass casualties and mass destruction.

Case Study – Khobar Towers Bombing (1996)

Overview

Shortly before 10:00 p.m. on the evening of June 25, 1996, a driver and one passenger drove a Datsun automobile into a public parking lot adjoining Khobar Towers building 131. This car acted as a scout vehicle and parked in a far corner of the lot. Soon after, a white four-door Chevrolet Caprice entered the parking lot and was staged for later use as escape transportation. The terrorists in the Datsun signaled that all was clear by blinking its lights. With that signal, a fuel truck converted into a truck bomb with an estimated 3,000-5,000 pounds of explosives approached the lot. The truck driver and his passenger entered the lot and backed the truck bomb against a perimeter fence in front of Khobar Towers building 131. After parking the truck, the truck driver and passenger quickly entered the back seat of the white Caprice. The Caprice, followed by the Datsun from the corner of the lot, sped away from the parking lot. Within minutes, the truck bomb exploded and devastated the north side of building 131, which was occupied by U.S. military members. The explosion killed nineteen U.S. military members and wounded 372 other Americans.[542] Many Saudi civilians and other third country citizens were injured in the attack.

The force of the explosion was so great that the effects heavily damaged or destroyed six high rise apartment buildings and shattered windows in virtually every other structure in the compound, leaving a crater in the ground 85 feet wide and 35 feet deep. The blast concussion was felt 20 miles away in the Persian Gulf state of Bahrain. At the time, this incident was the worst terrorist attack against Americans in more than a decade.[543]

Background

From the 1980s and leading up to the Khobar Towers bombing, Hizballah, or "Party of God," was the name used by a number of related Shia Islamic terrorist organizations operating in Saudi Arabia, Lebanon, Kuwait, and Bahrain. These Hizballah organizations were inspired, supported, and directed by elements of the Iranian government. Saudi Hizballah, also known as Hizballah Al-Hijaz, was a terrorist organization operating primarily in the Kingdom of Saudi Arabia. The group promoted, among other things, the use of violence against nationals

---

[542] U.S. District Court, Eastern District of Virginia, Alexandria Division. Grand Jury *Indictment* of 46 counts against named and unspecified terrorists charged in the Khobar Towers bombing attack of 25 June 1996, 13; available from http://www.fbi.gov/pressrel/pressrel01/khobar.pdf; Internet; accessed 10 February 2004.
[543] House National Security Committee, *Report on the Bombing of Khobar Towers* (14 August 1996), by Chairman Floyd D. Spence and Report, U.S. House National Security Committee, 1; Available from http://www.fas.org/irp/threat/saudi.pdf; Internet; accessed 10 February 2004.

and property of the United States located in Saudi Arabia. Because Saudi Hizballah was an outlaw organization in the Kingdom of Saudi Arabia, its members frequently met and trained in Lebanon, Syria, or Iran.[544]

In the 1990s, Saudi Arabia witnessed growing dissatisfaction by large segments of its population as social, economic, and political issues approached crisis proportion within the kingdom. Not surprisingly, religion provided a powerful influence in each of these other areas. The Saudi population was growing at a rapid pace, expectations and quality of life experienced in previous years was no longer feasible for many Saudi citizens due to changing economic conditions, and many Saudis considered the Saudi royal family an apostate regime due to the close relationship with the United States. [545]

U.S. military presence in Saudi Arabia had been a contentious issue with many Saudis. Many Saudi citizens, and other people of the region with an Islamic fundamentalist viewpoint, were particularly critical of this non-Muslim presence in a country that is home to two holiest places in the Islamic religion, Mecca and Medina. This concern was part of a larger cultural struggle in Saudi Arabia.[546]

Planning and Preparation

Saudi Hizballah began surveillance of Americans in Saudi Arabia in about 1993. Surveillance and reports continued to flow among Saudi Hizballah and officials in Iran. Potential targets included the U.S. Embassy in Riyadh and locales where Americans lived and worked. By 1994, Hizballah surveillance focused on eastern Saudi Arabia included Khobar Towers. In the months following, the terrorists recognized Khobar Towers as a lucrative target. The concentration of U.S. and coalition forces equated to between 2000 and 3000 people.[547] In mid-1995, terrorists began regular surveillance of Khobar Towers. Pre-attack surveillance was conducted with one vehicle. The vehicle was observed and reported ten times over 40 separate occasions of surveillance.

---

[544] U.S. District Court, Eastern District of Virginia, Alexandria Division. Grand Jury *Indictment* of 46 counts against named and unspecified terrorists charged in the Khobar Towers bombing attack of 25 June 1996, 2; available from http://www.fbi.gov/pressrel/pressrel01/khobar.pdf; Internet; accessed 10 February 2004.

[545] Joshua Teitelbaum and David Long, "Islamic Politics in Saudi Arabia," *The Washington Institute for Near East Policy, Policywatch:* Special Policy Forum Report Number 259, 9 July 1997, 1 to 3; available at http://www.washingtoninstitute.org/watch/Policywatch/policywatch1997/259.htm; Internet; accessed 19 February 2004. While Saudi Arabia attempted to balance modernization with its role as a protector of the holy places of Islam in the nation, U.S. military forces were an obvious secular presence in Saudi Arabia that offended many Saudi citizens. Aims of Islam and modernization were at odds. Disenchnated youth, ever increasing in size within the population, often vented their frustration with alliance or membership in radical, violent organizations. Young men recruited for the Saudi Hizballah would often be transported to Hizballah controlled areas in Lebanon for military training, weapons and explosives training, and indoctrination. Subsequent training and liaison occurred among terrorist members of the Saudi Hizballah and Lebanese and Iranian Hizballah organizations. Elements of the Iranian government sponsored forms of military training and other close association with terrorists.

[546] Alfred B. Prados, Congressional Research Service (CRS) Issue Brief for Congress, *Saudi Arabia: Current Issues and U.S. Relations*, 15 September 2003; Order Code IB93113, CRS-1.

[547] U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Wayne A. Downing, 16; available from http://www.fas.org/irp/threat/downing/unclf913.html; Internet; accessed 9 February 2004; Alain Gresh, "The unsolved mystery of a Saudi bomb attack," *Le Monde diplomatique*, September 1997, 2; available from http://mondediplo.com/1997/09/saudi; Internet; accessed 19 February 2004.

By early 1996, the terrorists were identifying locations to hide explosives. Explosives were eventually hidden in the area surrounding Khobar for use in the bombing attack. Of note, an attempt to smuggle explosives for this attack into Saudi Arabia was discovered and foiled on March 28, 1996 as a terrorist attempted to cross the Saudi Arabian border in a car. Saudi authorities confiscated 38 kilograms of plastic explosives hidden in the car and arrested the driver. Subsequently, Saudi investigators arrested several other terrorists. Nonetheless, Saudi Hizballah replaced these terrorists in the cell by May 1996 to replace or cover for an original group member for this attack. Additional large amounts of explosives were covertly collected and hidden in the vicinity of Khobar.

In early June over a two-week period, the terrorists used plastic explosives to convert a tanker truck into a bomb – a vehicle borne improvised explosive device (VBIED). Key members of the Saudi Hizballah and the attack cell met in Syria in mid-June 1996 to confirm tactical plans for the bombing. Early in the evening of June 25, 1996, the six members of the attack cell reviewed final preparations for the attack. Several hours later, Khobar Towers would become a terrorist incident of major proportion against U.S. military forces in Saudi Arabia.[548]

The Attack

On June 25, 1996, at approximately 10:00 p.m. Dhahran local time, a fuel truck laden with an improvised explosive device approached the northwest end of the Khobar Towers compound from the north and turned east onto 31st Street just outside the perimeter fence separating the compound from a public parking lot. The truck bomb had an estimated explosive power in the 20,000 pounds of TNT equivalent and probably larger class yield explosive.[549] The truck, and a car that it was following, continued to travel along the perimeter fence toward the northeast corner of the compound.

A U.S. military security guard, present at an observation site on the roof of Building 131, spotted the suspicious car and fuel truck as they continued to travel along the perimeter fence toward the eventual attack site. When the vehicles reached Building 131, they turned left, pointed away from the building, and stopped. The fuel truck backed up into the hedges along the perimeter fence, about 80 feet from, and directly in front of Building 131. When two men emerged from the truck, quickly entered the car, and sped away, the U.S. military security guard radioed the situation to the security desk and began, along with the other two guards on the roof, to evacuate the building.

Emergency evacuation procedures began for Building 131 as the three security personnel ran door to door, starting from the top floor and working their way down, knocking loudly on each door and yelling for the residents to evacuate. Three to four minutes after the truck had backed up against the perimeter fence, the bomb exploded, demolishing the entire front facade of the eight-story building.

---

[548] Ibid. 12 and 13.

[549] U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A* (31 October 1996) by Lieutenant General James F. Record, 54; available from http://www.fas.org/irp/threat/khobar_af/recordf.htm; Internet; accessed 9 February 2004.

Timely action on the part of the guards, who had only been able to work their way down several floors of the building, saved the lives of many residents of Building 131. Many residents evacuating the building were located in the building stairwells at the moment of the explosion. Given the injury and death caused by glass and other flying objects caused by the blast, the stairwells were probably the safest place to be at the time of bomb detonation.

However, the force of the blast destroyed building 131 and severely damaged five adjacent buildings. Most of the buildings in the U.S. occupied sector of the Khobar Towers complex suffered some degree of damage. Nineteen U.S. military members were killed with several hundred other people injured. Hundreds of Saudi and third country nationals living in the complex and immediate vicinity were also wounded. The bomb blast shattered windows throughout the compound and created a crater 85 feet wide and 35 feet deep. The blast was felt as far away as Bahrain, 20 miles to the southeast.

U.S. intelligence experts concluded that Americans were the targets of the terrorists. Although injury and death were extensive, an even greater number of casualties might have occurred had the driver positioned the truck differently against the fence and if at least one row of concrete barriers ["Jersey" barriers of the kind used in construction and on U.S. highways] had not been present to absorb or deflect part of the blast away from the lower level of building 131.

Senior leaders of the U.S. military unit, after consultation with engineers and investigators at the scene, concluded that this force protection measure helped to prevent the collapse of the lower floors of the building. Had the lower floors collapsed, the attack would have likely caused collapse of the entire building with a significantly larger number of casualties and fatalities.[550]

According to the terrorist plan, attack leaders immediately departed the Khobar Towers area and Saudi Arabia using false passports. Two terrorists remained in Saudi Arabia in their hometown. No Khobar Towers terrorists were captured immediately following the VBIED attack.

---

[550] House National Security Committee, *Report on the Bombing of Khobar Towers* (14 August 1996), by Chairman Floyd D. Spence and Report, U.S. House National Security Committee, 1 and 2; available from http://www.fas.org/irp/threat/saudi.pdf; Internet; accessed 10 February 2004.

Figure J-5. *Below*, **Photograph of Khobar Towers After the Bombing**
(Source: Report to the President and Congress on Protection of U.S. Forces Deployed Abroad (1996).)
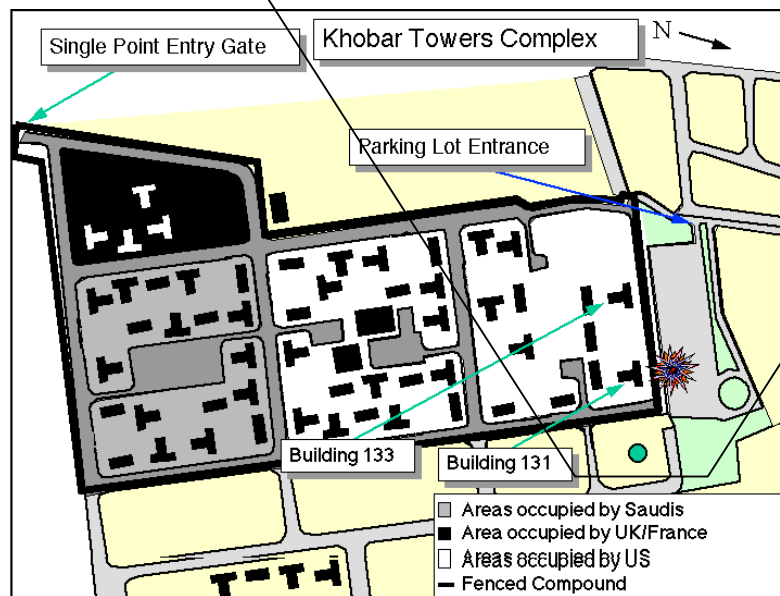
Figure J-6. *Above,* **Diagram Sketch of Khobar Towers and Bombing Site**
(Source: Report to the President and Congress on the Protection of U.S. Forces Deployed Abroad (1996).)

Supplemental Vignettes

Intelligence and Threat Warning

The U.S. Consul General in Dhahran at the time of the bombing stated, "No one really thought anything was going to happen in Dhahran. …[I] never had a piece of paper or anyone else outlining any particular threat."[551]   In general, the U.S. presence allowed allowed themselves to assume what the likely threats were, even in an absence of solid intelligence. A type of "tunnel vision" emerged that precluded an awareness of terrorist attack plans that were significantly greater than anything estimated.

The specific information U.S. officials in the region did have on terrorist capability consisted of evidence concerning the size of the 1995 car bomb terrorist attack in Riyadh that was equivalent to about 250 pounds of TNT, and numerous small pipe bombing incidents in nearby Bahrain. Senior U.S. officers in Saudi Arabia generally concluded that the upper limit of a terrorist bomb was no higher than what had been used in the 1995 car bombing. Likewise, the Saudis did not see terrorists using anything larger than the 1995 car bombing.

Other professional assessments did not estimate the damage potential of a bombing with the effects of the 1996 attack on Khobar Towers. The Regional Security Officer (RSO) at the U.S. Embassy in Riyadh related that a representative of his office had visited Khobar Towers prior to the bombing and was satisfied that the existing stand-off distance was adequate even though it was 20 feet less than the desired 100 foot State Department standard for fixed facilities. The RSO indicated that they would not have questioned an 80-foot stand-off distance even if the known threat had included a 1,000-pound bomb.

The Chief of the National Intelligence Support Team (NIST) in Riyadh indicated that they considered the threat to be a bomb the size of the one that exploded at Riyadh in 1995, "maybe 500 pounds but -- we never went above 1,000 pounds." Additionally, the U.S. Consul General in Dhahran stated, "the thought of a 20,000 or even 5,000 pound bomb driving up was pretty inconceivable."[552]

U.S. intelligence did not predict the precise attack on Khobar Towers. Commanders did have warning that the terrorist threat to U.S. military members and facilities was increasing. DOD elements in the theater had the authority, but were not exploiting all potential sources of information. Suspicious activities should have received more scrutiny. Human intelligence (HUMINT), had it been available, is probably the only source of information that could have provided the tactical details of a terrorist attack. In fact, a DOD report following the attack stated that the U.S. intelligence community must have the requisite authorities and invest more time, people, and funds into developing HUMINT against the terrorist threat.[553]

---

[551] U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A; Appendix 1, Comments Regarding the Downing Report* (31 October 1996) by Lieutenant General James F. Record, 51. Available from http://www.fas.org/irp/threat/khobar_af/recordap.htm; accessed 9 February 2004.

[552] Ibid. 50.

[553] U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Wayne A. Downing, 6; available from http://www.fas.org/irp/threat/downing/prefuncl.html; Internet; accessed 10 February 2004.

Security Measures in Effect

Although the U.S. intelligence community was providing coverage of terrorist and terrorist related activities, the intelligence support lacked in at least one key area. Intelligence did not provide timely tactical warning of the impending terrorist attack and the specific kind of attack on Khobar Towers. Yet, vulnerability analysis using general intelligence of threats resulted in improvements to physical security and force protection measures at Khobar Towers prior to the June 25, 1996 bombing. These actions did save lives and reduced injuries.[554]

Much of the force protection concentrated on precluding penetration of the complex perimeter by a car, truck, or suicide bomb. The commander responsible for the Khobar Towers complex was very proactive and aggressive in implementing improved security measures. Many complementing security measures were enacted such as an increased threat condition awareness, physical barriers and serpentine driving control patterns at checkpoints, restricted off-base travel, inspection procedures for parcels and commercial deliveries, and procedures for unannounced or suspicious visitors.[555] In the months preceding the Khobar Towers bomb attack, over 130 new security measures were implemented.[556]

The DOD task force report on the Khobar Towers bombing states a strong belief that "…to assure an acceptable level of security for U.S. forces worldwide, commanders must aggressively pursue an integrated systems approach to force protection that combines awareness and training, physical security measures, advanced technology systems, and specific protection measures tailored to each location. A comprehensive approach of common guidance, standards, and procedures will correct inconsistent force protection practices observed in the theater."[557]

Following the Khobar Towers terrorist attack, the U.S. Secretary of Defense directed a critical re-evaluation of U.S. force posture in the region, and empowered military commanders to examine mission tasks with force protection as an even more important consideration in its worldwide mission planning and operations.

Physical Site Vulnerabilities and Risk Assessment

Ten suspicious incidents, including four of possible surveillance, were reported by U.S. members in April, May, and June 1996. Many of the incidents were during the period of the Hajj. The Hajj, or pilgrimage to Mecca, is a central duty and one of the five pillars of Islam. However, U.S. military forces were concerned that this surge of thousands of worshippers

---

[554] U.S. Department of Defense. Report to the President. *The Protection of U.S. Forces Deployed Abroad* (15 September 1996) by Secretary of Defense William J. Perry, 5, 11 and 12; available from http://www.fas.org/irp/threat/downing/report_f.html; Internet; accessed 18 February 2004.
[555] U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A; Appendix 1, Comments Regarding the Downing Report* (31 October 1996) by Lieutenant General James F. Record, 11; available from http://www.fas.org/irp/threat/khobar_af/recordap.htm; Internet; accessed 9 February 2004.
[556] U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A* (31 October 1996) by Lieutenant General James F. Record, 44 and 47; available from http://www.fas.org/irp/threat/khobar_af/recordf.htm; Internet; accessed 9 February 2004.
[557] U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Wayne A. Downing, 5.

from around the world could be a likely period for extremist acts against U.S. presence in the vicinity of Islam's holy places in Saudi Arabia. The suspicious incidents in the vicinity of Khobar Towers were investigated by the U.S. military, Saudi military, and Saudi local police. Nothing in the investigations indicated an attack on Khobar Towers was imminent.

These incidents included one possible threat indicator − the suspected ramming of a "Jersey" barrier on the east perimeter of the Khobar Towers complex. Reported to Saudi authorities, they permitted U.S. military forces to secure the barriers by staking them into the ground. There were four incidents of possible surveillance, which were reported to local Saudi authorities for further investigation. These occurred on April 1, 4, 17 and 25, 1996, and all involved reports by U.S. military members of Middle Eastern men driving by the Khobar Towers compound, or parked and observing the compound. Of the five incidents, two were inconclusive and three were completely discounted.

These incidents were discussed with the Saudis, who did not view them as threatening. They attributed the incidents of possible surveillance to natural curiosity on the part of Saudi citizens about the activities of Americans inside the complex perimeter. A parking lot existed just outside the northern perimeter of Khobar Towers. Saudis used this lot as part of a community recreational area and to visit a nearby mosque. During the month-long period of the Hajj, it was normal for many people to congregate in this area during evenings. Most of the reported incidents took place during this time, and this may have caused the Saudi police to dismiss them as non-threatening. The Saudis said they had undercover security personnel in the area and they were not concerned.[558]

Host Nation Relationship

Saudi Arabia, as the host nation, retained sovereignty both inside and outside the complex at Khobar Towers. Saudi Arabian authorities permitted U.S. military forces latitude in security measures within the installation, but any permanent change to facilities required Saudi approval. Security internal to the complex was a shared responsibility by U.S. forces, coalition forces, and Saudi Arabian military police. Security outside the fence was a Saudi responsibility.[559] This tenuous sharing of force protection and limited ability to optimize security measures between the host nation, U.S. military forces, and the U.S. State Department caused significant challenges in the risk management of the Khobar Towers complex.

A January 1996 vulnerability assessment conducted by U.S. military forces identified the north perimeter fence area and the adjacent public parking lot as a significant weak point for three reasons: (1) the size and relative remoteness of the parking lot, (2) the visual obstruction that limits the ability of U.S. forces to identify an oncoming threat, and (3) access to the parking lot was uncontrolled and open to anyone. Recommendations included cutting back the vegetation, installing bollards (half buried steel pipes) connected by chain or cable along the

---

[558] U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A* (31 October 1996) by Lieutenant General James F. Record, 46 and 47; available from http://www.fas.org/irp/threat/khobar_af/recordf.htm; Internet; accessed 9 February 2004.

[559] U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A* (31 October 1996) by Lieutenant General James F. Record, 41; available from http://www.fas.org/irp/threat/khobar_af/recordf.htm; Internet; accessed 9 February 2004.

easement on the Saudi side of the fence or along the sidewalk on the U.S. side of the fence, reinforcing the existing concrete barrier line with one-inch steel cable, and parking heavy vehicles along the fence to limit high speed penetration of the installation. The vulnerability assessment noted the increased cooperation between U.S. and local Saudi police, and noted that Saudi military members would coordinate with local civilian authorities to increase the uniformed police presence outside the northwest and northeast fence lines.

An earlier 1995 vulnerability assessment addressed security measures to be taken around the perimeter fence, including the proper placement of concrete "Jersey" barriers, and removing or repositioning objects near the vegetation on the north perimeter to increase visibility. Comments noted successful efforts by the U.S. security police to establish liaison with the various local military and civilian police agencies and an increased willingness for cooperation between the U.S. military forces and local police.[560] The Saudi government, recognizing the need for U.S. military forces in the region since the Gulf War (1990-1991), encouraged a very urban presence of U.S. military forces. The Saudi royal family attempted to lessen the irritation of many Saudi to a "foreign presence" so near the holy places of Islam while simultaneously allowing the staging of U.S. military and coalition forces in their country. This tacit Saudi government aim exhibited itself in a methodical yet lethargic process for bolstering physical security measures suggested by U.S. military forces. In another practical limitation in an urban setting, expanding Khobar Towers security perimeters, emplacing more barriers, and clearing vegetation and foliage for better visibility along perimeters was counter to Saudi goals of minimizing Saudi citizen contact with U.S. forces. Expanding security distances in the area of the eventual attack site at Khobar Towers would have infringed on Saudi citizen access to a parking lot and park area near a local mosque.

Terrorist Tactics, Techniques, and Procedures

The terrorists organized in a cellular structure for their command and control. The Saudi Hizballah recruited from primarily young men of the Sh'ite faith. Cell members participating in this terrorist bombing came primarily from the same region in eastern Saudi Arabia, and in many cases, came from the same hometown. Loyalties such as a common religious earnestness, family and social relationships, and general dissatisfaction with Saudi government policies created a strong bond among members of this small group within the Saudi Hizballah. All cell members sequenced through deliberate phases of recruitment, indoctrination, and military-like training by the Saudi Hizballah.

Leaders, cadre, and supporters of this cell were focused on this particular mission and target. As a norm, interaction occurred usually between two to three cell members, but could involve up to six cell members with personal contact and oral exchanges. At times, written reports provided assessments and requirements. Occasionally, meetings and liaison occurred with the leader of the "military wing" of Saudi Hizballah or other Hizballah supporters. When three members of the cell were compromised and arrested by Saudi authorities during the preparation phase for the attack, replacement cell members were quickly assigned from the same hometown area. This change in cell members disrupted, but did not dismantle the attack plan. Compartmenting knowledge within the cell had benefited the terrorists as they proceeded with coordination meetings, received final guidance from Hizballah leaders,

---

[560] Ibid. , 49 and 50.

and set a timeline in motion to conduct the attack with a massive truck bomb at Khobar Towers.[561]

As noted earlier in the case study, planning and preparation included extensive surveillance. Pre-attack surveillance used one vehicle, which was observed and reported ten times of 40 separate uses as a surveillance means.[562] Reports and meetings with senior leaders of Saudi Hizballah supported planning in detail such as verifying the accuracy of a map of Khobar or the rehearsal of transporting explosives from Lebanon to Saudi Arabia.[563]

The DOD Task Force chartered to assess the Khobar Towers bombing estimated the bomb contained the equivalent of from 3,000 to 8,000 pounds of TNT, "most likely about 5,000 pounds." The Secretary of Defense commissioned a special study by the Defense Special Weapons Agency (DSWA). The DSWA report estimated the bomb was much larger with a likely yield of 20,000 to 30,000 pounds of TNT-equivalent.[564]

DSWA compared physical attributes of the Khobar Towers crater and blast with physical attributes of craters formed by vehicle bomb tests conducted under terrain conditions similar to those at Dhahran. DSWA determined that the "…'best' estimate for the Dhahran yield would be 11.5 tons or 23,000 pounds of TNT-equivalent explosive." DSWA compared the 5,000-pound TNT-equivalent yield estimate against the physical information known about the Khobar Towers crater and the crater information generated by the vehicle bomb tests. DSWA found that the 5,000-pound value implausible because it "implies a cratering efficiency greater than that produced by any known conventional explosive." DSWA's analysis of glass breakage from the Khobar Towers bombing resulted in an even larger estimated TNT-equivalent yield of 31,000 pounds. This figure was derived by plotting the actual number of windows broken at Khobar Towers on a computer-generated graph that depicts the number of glass patio doors that would be broken by the blast pressures generated by various TNT-equivalent yields.

A peer review by a panel of outside experts concluded the "DSWA analysis credibly supports the conclusion that the explosive power of the bomb was in the 20,000 pounds of TNT equivalent class and probably larger." The DSWA also noted that Building 133, located some 400 feet from the blast, sustained major structural damage. The weight of the evidence supports the DSWA estimate as to the size of the explosive.[565]

Terrorists recognize the media value of physical effects on a target but seek the psychological impact value of attack that often overshadows the act itself. The inability of enemies to

---

[561] U.S. District Court, Eastern District of Virginia, Alexandria Division. Grand Jury *Indictment* of 46 counts against named and unspecified terrorists charged in the Khobar Towers bombing attack of 25 June 1996, 3 to 12; available from http://www.fbi.gov/pressrel/pressrel01/khobar.pdf; Internet; accessed 10 February 2004.

[562] Department of State, Bureau of Diplomatic Security, *State Department Diplomatic Security Surveillance Detection Program Course of Instruction* [CD-ROM], (Washington, D.C., October 1999).

[563] U.S. District Court, Eastern District of Virginia, Alexandria Division. Grand Jury *Indictment* of 46 counts against named and unspecified terrorists charged in the Khobar Towers bombing attack of 25 June 1996, 7 to 9; available from http://www.fbi.gov/pressrel/pressrel01/khobar.pdf; Internet; accessed 10 February 2004.

[564] U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A* (31 October 1996) by Lieutenant General James F. Record, 53; available from http://www.fas.org/irp/threat/khobar_af/recordf.htm; Internet; accessed 9 February 2004.

[565] Ibid. 54.

challenge U.S. and allied military power directly will likely lead to their asymmetric use of force to deter U.S. initiatives, attack forward deployed forces, and attempt to drive a wedge between the United States and its coalition partners. Terrorist attacks are intended to weaken U.S. resolve to maintain a force presence in threatened regions and to influence U.S. public and congressional opinion. Asymmetric use of force could include employment of weapons of mass destruction. The target will be U.S. citizens. Creation of casualties, whether from attacks like the one on Khobar Towers or more discrete attacks designed to establish a pattern of insecurity and helplessness, allows an enemy to demonstrate U.S. vulnerabilities at overseas locations and achieve political aims through indirect means.[566]

The Immediate Aftermath

International media attention spotlighted the terrorist attack on U.S. military forces in the Kingdom of Saudi Arabia. Terrorists achieved objectives of notoriety with a worldwide audience and significant psychological trauma of mass casualties and horrific property damage. U.S. military forces suffered terrible injuries and loss of life; similar injuries and damage occurred to the surrounding Saudi community. U.S. military forces lost prestige when a compound considered relatively safe was easily attacked and devastated with a large bomb. The royal family of Saudi Arabia lost prestige because of its inability to prevent such a terrorist attack that affected Saudi citizens, civilians and government workers from other countries, and the U.S. military presence as their invited temporary guests. Regional and world attention weakened Saudi royal family prestige, from an Islamic perspective, due to the presence of a non-Muslim military force in its country of holy places for the Islamic faith.

Case Discussion Questions

Intelligence and Threat Warning?

What suspicious activities preceding the bombing attack might have indicated the tactical targeting of the Khobar Towers complex in an operational level U.S. intelligence estimate?

Security Measures in Effect?

How did Saudi and U.S. force protection measures encourage the terrorists to select the Khobar Towers complex for attack?

What does the proximity of distance of the Khobar Towers building 131 to the perimeter of the residential complex suggest in force protection vulnerabilities?

Physical Site Vulnerabilities and Risk Assessment?

Why did terrorists detonate the VBIED at the specific point of the Khobar Towers complex?

Given the same bomb (VBIED) and scenario of Khobar Towers, how could terrorists have increased mass casualty effects?

---

[566] U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Wayne A. Downing, 5; available from http://www.fas.org/irp/threat/downing/unclf913.html; Internet; accessed 9 February 2004.

Host Nation Relationship?

How could the U.S. military unit chain of command and local Saudi security forces have cooperated more effectively in collective security of the Khobar Towers complex?

What impact did the urban location of Khobar Towers and a Saudi government aim of minimizing Saudi citizen contact and visibility with U.S. military forces have in hampering progressive physical security measures?

Terrorist Tactics, Techniques, and Procedures?

Why did the terrorist group choose the Khobar Towers as a principal target in Saudi Arabia?

How did the terrorist group structure itself, communicate, and operate during the phases of planning and execution of the Khobar Towers bombing attack?

Assessment

Intelligence gaps left the U.S. military organization and its leaders at the Khobar Towers complex largely unaware of the magnitude of the threat they faced. Intelligence support fell short in at least three ways. First, available intelligence was devoid of specific knowledge of terrorist and dissident activity inside Saudi Arabia. As a result, assessments were incomplete. Second, intelligence analysis did not examine vulnerabilities in the context of capabilities greater than those already demonstrated in the 1995 bombing in Riyadh. Formal threat assessments appear to have remained reactive to events. Third, intelligence assessments did not acknowledge their own limitations. They did not communicate a level of uncertainty that should have been appropriate considering the lack of specific knowledge available and the difficulty of understanding the complex environments of Saudi society. Based on such intelligence assessments, U.S. commanders in the theater of operations and in the region of Riyadh likely had a false sense of appreciating the level of threat they faced and the requisite level of security required to protect U.S. forces.

Problems stemming from such intelligence failures were further complicated by the organizational and operational shortcomings of the U.S. military mission characterized and conducted as a temporary mission. The provisional U.S. organization lacked continuity, cohesion, and adequate personnel resources. In particular, short-tour rotations — where 10 percent of the command was new to the theater every week — created an unacceptable level of unit instability. This constant turnover of people in duty positions placed a significant knowledge and coordination burden on officers and enlisted members of the command. The high turnover rate hampered any practical ability for U.S. military leaders to build a relationship of trust with their Saudi host.

Deference to Saudi cultural sensibilities, religious concerns, and domestic political concerns discouraged U.S. commanders in the field from aggressively pursuing more expansive security measures. While important, consideration of host country cultural sensitivities or domestic politics should not have allowed any compromise to protection of U.S. forces, particularly in regions where a growing threat of terrorism focused against Americans.

The combination of situational factors resulted in terrorists being able to identify target site vulnerabilities, conceive a plan to attack a point of weakness, conduct methodical preparation, react to disruption of terrorist group membership, and effectively attack the designated target to achieve their objectives against the Saudi government and U.S. military forces.

Resources

Gresh, Alain. "The unsolved mystery of a Saudi bomb attack." *Le Monde diplomatique.* September 1997, 2. Available fro http://mondediplo.com/1997/09/saudi. Internet. Accessed 19 February 2004.

Prados, Alfred B. Congressional Research Service (CRS) Issue Brief for Congress. *Saudi Arabia: Current Issues and U.S. Relations*, 15 September 2003. Order Code IB93113.

Teitelbaum, Joshua and David Long. "Islamic Politics in Saudi Arabia." *The Washington Institute for Near East Policy, Policywatch:* Special Policy Forum Report Number 259, 9 July 1997, 1 to 3. Available at http://www.washingtoninstitute.org/watch/Policywatch/policywatch1997/259.htm; Internet; Accessed 19 February 2004.

U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A* (31 October 1996) by Lieutenant General James F. Record. Available from **http://www.fas.org/irp/threat/khobar_af/recordf.htm**; Internet; Accessed 9 February 2004.

U.S Air Force. *Independent Review of the Khobar Towers Bombing, Part A; Appendix 1, Comments Regarding the Downing Report* (31 October 1996) by Lieutenant General James F. Record. Available from **http://www.fas.org/irp/threat/khobar_af/recordap.htm**; Internet; Accessed 9 February 2004.

U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Wayne A. Downing. Available from **http://www.fas.org/irp/threat/downing/downltr.html**; Internet; Accessed 10 February 2004.

U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Wayne A. Downing. Available from **http://www.fas.org/irp/threat/downing/prefuncl.html**; Internet; Accessed 10 February 2004.

U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Wayne A. Downing. Available from **http://www.fas.org/irp/threat/downing/unclf913.html**; Internet; Accessed 9 February 2004.

U.S. Department of Defense. Report to the President. *The Protection of U.S. Forces Deployed Abroad* (15 September 1996) by Secretary of Defense William J. Perry. Available from **http://www.fas.org/irp/threat/downing/report_f.html**; Internet; Accessed 18 February 2004.

U.S. Department of State, Bureau of Diplomatic Security, *State Department Diplomatic Security Surveillance Detection Program Course of Instruction* [CD-ROM], (Washington, D.C., October 1999).

U.S. Department of State. International Information Programs Bulletin. *Justice Department on Khobar Towers Explosion Indictments* (21 June 2001). Available from **http://usinfo.state.gov/topical/pol/terror/01062102.htm**; Internet; Accessed 10 February 2004.

U.S. District Court, Eastern District of Virginia, Alexandria Division. Grand Jury *Indictment* of 46 counts against named and unspecified terrorists charged in the Khobar Towers bombing attack of 25 June 1996. Available from **http://www.fbi.gov/pressrel/pressrel01/khobar.pdf**; Internet; Accessed 10 February 2004.

U.S. House National Security Committee. *Report on the Bombing of Khobar Towers* 14 August 1996). Statement of Chairman Floyd D. Spence and Staff Report. Available from **http://www.fas.org/irp/threat/saudi.pdf**.; Internet; Accessed10 February 2004.

Walsh, Elsa. "Louis Freeh's Last Case." The New Yorker, 14 May 2001. Available from **http://www.newyorker.com/printable/?archive/010924fr_archive06**; Internet; Accessed 12 February 2004. (*Note:* This magazine article presents an interesting complement to the U.S. government sources cited in this case study. The article author recounts the frustrating political and judicial coordination that confronted Federal Bureau of Investigation Director Louis Freech, during his FBI investigation of the Khobar Towers terrorist bombing.)

Case Study – USS *Cole* (2000)

Abstract: USS *Cole*

The maritime attack on the USS *Cole* by two individuals in a small boat, loaded with explosives, demonstrated an effective means of terrorism against U.S. military forces. When the suicide terrorist attack occurred, the bomb explosion next to the ship caused 17 crewmember deaths, wounded 39 other crewmembers, and seriously damaged the ship. Two terrorists were also killed in the explosion. As stated by the President to the U.S. Congress shortly after the terrorist attack:

The "boat bombing" of the USS *Cole* introduced a new tactic of terrorism attack against a U.S. warfighting ship in a contemporary operational maritime setting. This case study presents an unclassified summary of U.S. observations and findings of U.S. intelligence shortfalls, U.S. force protection vulnerabilities, U.S. and host nation operational sensitivities, and the calculated strategy and tactic of a specific terrorist act.

Figure J-8. *Above,* **USS *Cole* After the Attack**
(*Source*: **http://www.chinfo.navy.mil**)

Figure J-7. *Left,* **USS *Cole* (DDG 67)**
(*Source*: http://federalvoice.dscc.dla.mil)

Terrorists have the luxury of searching for a single vulnerability. Timing and method are tools of terrorist choosing and further complicate risk management and force protection of a target selected by terrorists. A primary underlying aim of terrorism is a demoralizing psychological effect on the target population and its leaders, often with explicit media coverage of mass casualty or mass destruction effects, to erode resolve and enhance terrorist objectives.

Introduction

The 12 October 2000 attack on USS *Cole* in the port of Aden, Yemen, took advantage of a seam in the fabric of U.S. efforts to protect naval forces during an "in-transit" phase of deployment. The USS *Cole*[567] (DDG 67) is an Aegis missile equipped, Arleigh Burke class, destroyer. As a result of the attack, attention focused on implementing ways to improve U.S. policies and practices for deterring, disrupting, and mitigating terrorist attack on U.S. maritime forces in transit.

U.S. military forces support engagement elements of both the National Security Strategy and the National Military Strategy. This means continuous transit of U.S. ships, aircraft and military units. U.S. military forces operate on land, in the air, and on the seas in a world environment characterized by unconventional and transnational threats. Sovereign waterways, the high seas, or even a temporary berthing site are all possible locations for maritime terrorism.[568] Assessing a chronology of terrorist group activities verifies a dedicated motivation and deliberate planning and execution cycle that applied phases of reconnaissance and surveillance, specific target selection, staging and rehearsal, preparation, attack; and although this was a deliberate suicide attack, escape plans for terrorist support elements following the bombing.

Learning Objectives

Learning objectives focus on analyzing case study information in order to synthesize and evaluate the insight of reflective experiences, discern patterns of terrorist method and means, and determine likely trends in future terrorist activities. Comparing and contrasting conditions, circumstances, and asymmetric options available to the terrorist will enhance judgment to recognize vulnerabilities, identify threats, and minimize the ability of terrorism to impact on accomplishing a friendly force mission.

The objectives for this case study are:

- Describe intelligence indicators that might have created a more effective tactical estimate of terrorist intention and capability in the USS *Cole* bombing.

- Understand the motivation of Yemeni extremists and their associated support groups for choosing the USS *Cole* as a terrorist target of high value.

- Recognize U.S. vulnerabilities to force protection measures at the USS *Cole* refueling site that terrorists optimized in the bombing attack.

---

[567] Raphael Perl and Ronald O'Rourke, *"Terrorist Attack on USS Cole: Background and Issues for Congress,"* Congressional Research Service, The Library of Congress, Order Code RS20721, 1, 30 January 2001; available from http://news.findlaw.com/cnn/docs/crs/coleterrattck13001.pdf; Internet; accessed 5 April 2004.
[568] Department of Defense, *DoD USS Cole Commission Report* (9 January 2001) by U.S. Army Gen. (Ret) William Crouch and U.S. Navy Adm. (Ret) Harold Gehman, open-file report, U.S. Department of Defense, 1 (Washington, D.C., 9 January 2001); available at http://www.fas.org/irp/threat/cole.html; Internet; accessed 16 February 2004.

- Explain the terrorist organizational structure and tactics, techniques, and procedures (TTP) used for the USS *Cole* bombing.

- Deduce a trend for terrorist acts with the objective of an increased combination for mass casualties and mass destruction.

Case Study - USS *Cole* (2000)

Overview

U.S. military presence in the Mideast region demonstrates regional engagement while U.S. air, sea, and land forces deter aggression by anyone who would threaten U.S. critical national interests. In 2000, USS *Cole* was proceeding to join a carrier battle group in the Gulf region that formed a key part of an immediate ready force. This began with the ship's deployment from Norfolk on August 8th. The trans-Atlantic Ocean crossing lasted until August 20th when the ship and crew started conducting operations in the Mediterranean Sea. These operations, along with several port visits, lasted from August 20th until October 9th. Then, USS *Cole* transited the Suez Canal in order to conduct maritime operations in the northern Arabian Gulf in support of enforcing United Nations Security Council Resolutions.

Yemen plays a key part in the ability for U.S. and coalition maritime forces to operate in the region. Yemen controls the eastern side of the Bab al Mandeb choke point at the southern end of the Red Sea, and is geo-strategically positioned approximately 1400 miles south of Suez and 1400 miles southwest of the Strait of Hormuz.[569]

Given the pending 3300-mile movement from the Suez Canal to the Northern Arabian Gulf, USS *Cole* required refueling. According to U.S. Navy policy, an oiler [fuel ship] does not accompany a single ship during transits, so the decision was made that USS *Cole* would conduct a brief stop for fuel (BSF) in Aden, Yemen.

The operational requirement to refuel necessitated the development of: (1) a force protection plan for the refueling operation at Aden, (2) a logistics request for husbanding services at the port, and, (3) a request for the necessary diplomatic clearances. USS *Cole* met these requirements and continued the route down the Red Sea entering the port of Aden on October 12th. She moored to the starboard side of a refueling platform at 8:49 a.m. (local Yemen time).[570]

---

[569] Tommy Franks, "General Tommy Franks Testimony on USS *Cole*" [database on-line] (Washington, D.C., 25 October 2000); 5; available from http://www.fas.org/man/dod-101/sys/ship/docs/man-sh-ddg51-001025zd.htm; Internet; accessed 5 April 2004.
[570] Ibid., 7.
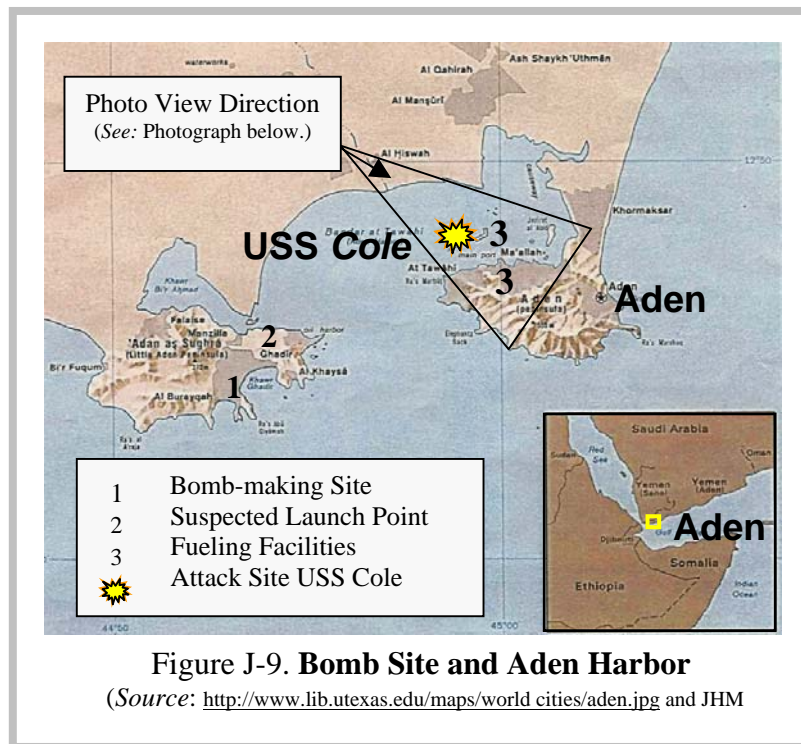
Figure J-9. **Bomb Site and Aden Harbor**
(*Source*: http://www.lib.utexas.edu/maps/world cities/aden.jpg and JHM

Figure J-10. **Aerial View of Port at Aden**
(*Source*: http://www.chinfo.navy.mil/navpalib)

Background

The U.S. Central Command (USCENTCOM) area of operations is a large, dangerous, and complex region, consisting of 25 countries, with over half a billion people from a variety of

ethnic and religious backgrounds. The region is historically unstable, yet remains vital to U.S. national interests. It contains vast energy resources, key air and sea lines of communication, and critical maritime choke points. Economic and political disruptions can have profound global consequences. Sources of instability within the region include hegemony, terrorism, proliferation of weapons of mass destruction, and ballistic missiles. Conflict is a norm in this region. Between USCENTCOM forming in 1983 as a U.S. military command and the USS *Cole* bombing in 2000, USCENTCOM responded to crises on 23 occasions.[571]

U.S. Navy ships began making brief stops for fuel at Aden in January 1999. The decision to go into Aden for refueling was based on operational as well as geo-strategic factors and included an assessment of the terrorist and conventional threats in the region. The Horn of Africa was in great turmoil in 1998, as exemplified by continuing instability in Somalia, the U.S. Embassy bombings in Kenya and Tanzania, an ongoing war between Ethiopia and Eritrea, and an internal war in Sudan. In December 1998, combat strikes were conducted against Iraq for non-compliance with UN Security Council Resolutions. As of December 1998, 14 of the 20 countries in the USCENTCOM area of responsibility (AOR) were characterized as "High Threat" countries.

Djibouti, which had been the U.S. Navy refueling stop in the Southern Red Sea for over a decade, began to deteriorate as a useful port because of the Eritrea-Ethiopia war. This war caused increased force protection concerns for our ships, as well as congestion in the port resulting in operational delays.

Aden, Yemen was seen as a viable alternative for refueling operations. Although the terrorism threat is endemic in this region. While the intelligence community and USCENTCOM regularly monitored the threat situation of the region and locales, no specific threat information or warning for Yemen or Aden indicated a pending terrorist attack on a U.S. warship, however, since the U.S. Navy began refueling operations in Aden in January 1999, U.S. Navy ships had conducted 27 brief stops for fuel, two port visits, and one logistics visit without incident. Nonetheless, Yemen was acknowledged as a high threat environment.[572]

Planning and Preparation

A U.S. Federal Indictment issued in May 2003, describes a primary timeline of terrorist planning and preparation in 1999 and 2000 for the October 2000 terrorist attack. A U.S. Federal grand jury indicted two Yemeni nationals for plotting the October 2000 attack on the USS *Cole* in the harbor of Aden, Yemen. The Indictment alleges that Usama bin Laden's 1998 fatwa authorizing the killing of Americans motivated the defendants to conduct the terrorist attack on the USS *Cole*. Although Usama bin Laden may not be linked to the specific direction of the USS *Cole* attack, several links exist among al Qaeda operatives and the terrorists in this attack.

This Indictment charges Jamal Ahmed Mohammed Ali al-Badawi and Fahd al-Quso with various terrorism offenses, including murder of U.S. nationals and murder of U.S. military personnel. Badawi was also charged with attempting, with co-conspirators, to attack the U.S.

---

[571] Ibid., 4.
[572] Ibid., 6 and 7.

destroyer USS *The Sullivans* in January 2000, while it was refueling in the port of Aden. The defendants, both alleged to be longtime al Qaeda associates, remain at large overseas. They had been in custody in Yemen until they escaped from prison in early 2003.

The table in this case study displays a timeline and series of actions leading to the terrorist attack on the USS *Cole*. Although not known by U.S. authorities at the time of the USS *Cole* attack, terrorists had attempted to attack USS *The Sullivans* on January 3, 2000, while the ship was berthed for servicing in Aden Harbor. Terrorists loaded a boat with explosives and launched the boat from the beach. However, the attack was aborted when the boat sank under the weight of the explosives. The May 2003 Federal Indictment alleges that the terrorists salvaged the explosives, refit the boat, and began plotting another attack.

Badawi was a key al Qaeda operative in Aden recruited by terrorists closely associated with Usama bin Laden. Badawi assisted in procuring safehouses in Aden for terrorists, obtained the attack boat, and provided the trailer and truck used to tow the boat to Aden harbor. Quso facilitated the plot to attack USS *Cole* and prepared to film the attack from an apartment on the hills overlooking Aden Harbor. Among several unindicted co-conspirators, one is Tafiq Muhammed Saleh Bin Roshayd Bin Attash, also known as Khallad, and Abdul Rahim Mohammed Hussein Abda Al-Nasheri, who are alleged to be veteran students and teachers in the al Qaeda terrorist camps in Afghanistan. Saif al Adel, a member of al Qaeda's military committee, who allegedly participated in the planning of these attacks, is also indicted in the East Africa embassy bombing case. Badawi, at the direction of Khallad and Nasheri, went to Saudi Arabia, purchased a boat large enough to carry explosives, and a trailer and truck to tow the boat, and secured a safehouse in Aden to hide the boat until the attack.

Raed Hijazi was the man in charge of terrorist training for the USS *Cole* attack. According to U.S. sources, Raed Hijazi is a former Boston [USA] taxi driver and an American citizen of Palestinian origin. Jordanian security officials link him as a close associate of Mohammed Abu Zubayda, a member of Bin Laden's inner circle. Hijazi was arrested in Syria at the end of 2000 and later transferred to Jordan where he had been sentenced to death in his absence for involvement in Bin Laden's alleged millennium plot, which included targets in Jordan and the U.S. Some evidence exists that the suicide attack in Aden Harbor was originally planned as part of the al Qaeda millennium plot.[573]

According to the U.S. Federal Bureau of Investigation (FBI), Khalid al-Midhar, a hijacker aboard the plane that crashed into the Pentagon on September 11 had earlier been observed on a surveillance video in Malaysia meeting an unnamed man who is suspected of involvement in the USS *Cole* attack. According to Abd al-Karim al-Iryani, who was Yemen's prime minister at the time of the attack, "Khalid al-Midhar was one of the *Cole* perpetrators, involved in preparations...He was in Yemen at the time and stayed after the *Cole* bombing for a while, then he left."[574] Association of al Qaeda operatives to members of this terrorist act in Aden Harbor appears conclusive.

---

[573] "Attack on the USS *Cole*," Yemen Gateway [database on-line]; available from http://www.al-bab.com/yeman/cole1.htm; Internet; accessed 6 April 2004.
[574] Ibid.

Table J-2. Timeline for USS *Cole* Maritime Bombing
"On or About Dates"[575]

Chronology	Event
Spring 1999	NASHERI[576] enlists BADAWI[577] with a letter from KHALLAD[578] to assist in a terrorist operation.
Summer 1999	BADAWI locates a residence in Aden that provides privacy.
Summer 1999	NASHERI leases property in Aden for six-month period.
Summer 1999	NASHERI directs BADAWI to procure a boat and a truck to tow the boat to Aden Harbor.
Summer 1999	NASHERI and other individuals secure a boat on the property.
3 January 2000	NASHERI and other individuals transport an explosives-laden boat from the property to the Aden Harbor beachfront.
3 January 2000	NASHERI and other individuals launch an explosives-laden boat with intention of bombing USS *The Sullivans* in Aden Harbor. The explosives-laden boat sinks shortly after launching.
4 January 2000	NASHERI and other individuals return to the beachfront and salvage the sunken boat and explosives.
January 2000	QUSO[579] and NIBRASS[580] travel to Bangkok, Thailand. QUSO is directed to shave and wear western-style clothing so he doesn't attract attention on trip. They deliver approximately $36,000 to KHALLAD in Bangkok, Thailand.
Spring 2000	NASHERI informs BADAWI of aborted attempt to bomb USS *The Sullivans*, and discusses ongoing plot to attack U.S. naval ship and comply with Usama Bin Laden edict to drive American forces from the Arabian Peninsula.
Summer 2000	HASAN[581] leases a lodging to act as a safehouse in Aden.
Summer 2000	HASAN leases an apartment to act as an observation post perched on the hills overlooking Aden harbor.
Summer 2000	KHALLAD and NASHERI meet with Usama Bin Laden and other individuals in Afghanistan. NASHERI tests explosives while in Afghanistan.

[575] U.S. District Court, Southern District of New York. Indictment S12 98 Cr. 1023 (KTD). United States of America, Plaintiff, vs. Jamal Ahmed Mohammed Ali Al-Badawi and Fahd Al-Quso, Defendants; available from http://news.findlaw.com/hdocs/docs/cole/usalbadawi051503ind.pdf;
Internet; accessed 5 April 2004.
[576] Abdul Rahim Mohamed Hussein Abda Al-Nasheri, aka NASHERI. S12 98 Cr. 1023
[577] Jamal Ahemd Mohammed Ali Al-Badawi, aka BADAWI. S12 98 Cr. 1023
[578] Tafiq Muhammed Saleh Bin Roshayd Bin Attash, aka KHALLAD. S12 98 Cr. 1023
[579] Fahd Al-Quso, aka QUSO. S12 98 Cr. 1023
[580] Ibrahim Al-Thawar, aka NIBRASS. S12 98 Cr. 1023
[581] Hassan Awadh Al-Khami, aka HASAN. S12 98 Cr. 1023

Summer-Fall 2000	NASHERI and other individuals refit the boat that had sunk in January 2000, and test the explosives that had sunk in the boat.
September 2000	BADAWI trains QUSO to film the planned attack on a U.S. ship in Aden Harbor from an area apartment and vantage point.
Sept - Oct 2000	BADAWI provides QUSO with a pager, and informs QUSO that he'll receive a predetermined code that would indicate the imminent attack on a U.S. ship. QUSO would depart to the area apartment and vantage point.
Sept – Oct 2000	KHALLAD returns from Yemen to Afghanistan.
October 12, 2000	NIBRASS, HASAN, and other individuals tow the explosives-laden boat with a truck to the Aden Harbor beachfront.
October 12, 2000	QUSO departs his residence to go to the vantage point.
October 12, 2000	NIBRASS and HASAN board the explosives-laden boat and launch the boat-bomb in the direction of the USS *Cole*.
October 12 11:18 a.m.	NIBRASS and HASAN offer friendly gestures to observing crew members of the USS *Cole*, and steer the boat alongside USS *Cole*. **Boat-bomb detonates next to USS *Cole*.**[582] 17 U.S. sailors killed; 39 U.S. sailors wounded. The terrorists NIBRASS and HASAN killed in suicide attack. The blast leaves a 40-foot diameter hole in ship's side with the ship in jeopardy of sinking.

The Attack

As the USS *Cole* entered Aden harbor, the ship did not dock at the quayside. Refueling took place at a water-borne platform known as a dolphin. This fuel transfer point is a commercially run Yemeni operation and lies about 600 meters offshore. The U.S. Navy contracted for such refueling operations.

After verifying the refueling alignment, refueling operations commenced at 10:31 a.m. At 11:18, two suicide attackers detonated their explosives-laden boat against the side of the USS *Cole*.[583] The small boat was probably loaded with between 400 to 700 pounds of explosives, and the blast blew a 40-foot hole in the side of the USS *Cole*. U.S. analysis of explosive residues found at the blast site indicates that the terrorist bombers used C-4.

The Immediate Aftermath

Shortly after the boat suicide attack, three groups claimed responsibility for the Aden attack – the Islamic Army of Aden-Abyan previously unknown in Yemen, the Army of Mohammed, and the Islamic Deterrence Forces (IDF). The Army of Mohammed also claimed responsibility for bombing the British embassy in Sana'a the following day. The Islamic Army has previously claimed responsibility for several incidents in Yemen which turned out not to have been terrorist acts.

---

[582] Franks, 7.
[583] Ibid.

The IDF's statement said the attack was in "defence [defense] of the honour [honor] and dignity of the Islamic nation and to avenge the blood of the oppressed Muslim nation in Palestine with the blessing of the American regime for that enemy … This operation will not be the last, as such attacks will continue against our enemy, and the enemy of our Arab and Muslim nation: America and its artificial Zionist entity in Palestine."[584]

In stark contrast to terrorist announcements, many governments and allied military forces provided immediate responsive support during the aftermath of the USS *Cole* bombing. The Government of Yemen provided initial medical support and security forces to protect U.S. Government officials arriving in the area. France and Djibouti helped with initial medical evacuation and treatment. Royal Navy ships HMS *Marlborough* and HMS *Cumberland* provided damage control and other assistance. Expedited overflight clearances were approved, as well as the use of air bases from Saudi Arabia, Egypt, Bahrain, Oman, Kuwait, and Qatar.[585]

Supplemental Vignettes

Intelligence Threat and Warning

The threat situation was monitored regularly in Yemen and throughout the U.S. military area of responsibility (AOR). The U.S. intelligence community and USCENTCOM considered this area a High Threat environment. A number of threat assessments had been conducted in the port and throughout the area. However, leading up to the attack on USS *Cole* on October 12th, no specific threat information for Yemen or for the port of Aden was reported that would cause a change to the assessment.[586]

The *DOD USS Cole Commission Report* (9 January 2001) states that intelligence priorities and resources have shifted from a Cold War focus to new and emerging threats only at the margins. Contemporary events indicate that intelligence resources need to be reprioritized for collection and analysis, including human intelligence and signal intelligence, against terrorism. Intelligence production must be refocused and tailored to safeguard transiting units in order to mitigate the terrorist threat. Furthermore, a requirement exists for an increase in counterintelligence (CI) resources dedicated to combating terrorism and development of clearer CI assessment standards.[587]

The investigation by the DOD Commission identifies that the commanding officer of the USS *Cole* did not have the specific intelligence, focused training, appropriate equipment or on-scene security support to effectively prevent or deter such a determined, pre-planned assault on his ship.[588]   In-transit units require intelligence support tailored to the terrorist threat in their immediate area of operations. This support must be dedicated from a higher echelon with

---

[584] "Attack on the USS *Cole*," Yemen Gateway [database on-line]; available from http://www.al-bab.com/yeman/cole1.htm; Internet; accessed 6 April 2004.

[585] Franks, 3.

[586] Ibid., 6.

[587]*DoD USS Cole Commission Report*, 1.

[588] Department of Defense News Release Archive, "DoD News: Navy Announces Results of Its Investigation on USS *Cole*;" available from http://www.defenselink.mil/releases/2001/b011192001_bt031-01.html; Internet; accessed 11 February 2004.

focused analysis and tailored production.[589] Independent transiting units must be better trained and resourced to submit appropriate requests for information to force intelligence organizations. This will allow these intelligence activities to be responsive to the transiter's anti-terrorism/force protection (AT/FP) requirements.

Security Measures in Effect

Military sources and several news agencies reviewed the actions conducted, as well as actions not conducted, by the ship and crew as the USS *Cole* entered the harbor. Clearly, the terrorists were able to observe patterns that previous ships displayed during their visits to Aden Harbor. For example, terrorists could easily see if U.S. forces attempted to control the movement of small boats near a warship in the harbor, as well as what crewmember presence and actions were visible on deck.[590]

From post-attack analysis recommendations, U.S. military forces must create an integrated system of training that produces a unit that is clearly and visibly ready, alert and capable. To achieve this level of AT/FP proficiency, this type of training must be elevated to the same priority as primary mission training.[591] DOD and Service guidance on the content of anti-terrorism/force protection Level III commander-type training must be more definitive if senior field grade officer (O-5 and O-6) levels are to execute their AT/FP responsibilities.[592] Demonstrating visible force protection by transiting units can more effectively deter terrorist attacks.[593]

Host Nation Relationship

While classifying the diplomatic clearance and logistics requirement process may improve the operational security of transiting units, it is not practical due to the commercial nature of the process. Local providers of goods, services, and transportation must be employed to support these type operations. Consequently, they must be evaluated in ways that enhance the AT/FP posture of the in-transit unit.[594] According to Admiral Vern Clark, Chief of Naval Operations, refueling arrangements had been made 10 to 12 days earlier through the U.S. Embassy in Yemen - a standard procedure.[595] Implementing proactive AT/FP measures must mitigate the real and potential effect of public knowledge of visits by U.S. military forces.

> **"As I have previously stated in testimony before this [Senate and House Armed Services] committee, 'Our men, women, DOD civilians, and Diplomats in the region are under constant observation, and, in some**

---

[589] *DoD USS Cole Commission Report*, 7.
[590] "Attack on the USS *Cole*," Yemen Gateway [database on-line]; available from http://www.al-bab.com/yeman/cole1.htm.
[591] *DoD USS Cole Commission Report*, 2
[592] Ibid., 9.
[593] Ibid., 6.
[594] Ibid., 8.
[595] "Attack on the USS Cole," Yemen Gateway [database on-line]; available from http://www.al-bab.com/yeman/cole1.htm.

> **cases, being stalked, everyday, 24-hours-a-day, because the terrorist threat in this region is very real.'"**[596]

> General Tommy Franks
> Commander
> U.S. Central Command

The U.S. criminal investigation into the attack was led by the U.S. FBI, which immediately deployed nearly 200 agents and technicians to begin the arduous work of putting together the pieces of the puzzle and finding who was responsible. The FBI worked closely with officials from the Naval Criminal Investigation Service, NYPD [New York Police Department] officers from the New York Joint Terrorism Task Force, and Yemeni investigators.[597]

Yemen, while recognizing that it had to cooperate to some extent for the sake of its relations with the U.S., insisted on maintaining its independence and sovereignty in a case which had occurred within its national territory. Investigative disputes between Yemen and the U.S. resulted in a phone call from President Bill Clinton to President Salih. On November 6, State Department spokesman Richard Boucher said: "We got good cooperation during the first phase. ... We're in discussions with them [the Yemenis] on the modalities of how we will cooperate further in the future..."

Terrorist Tactics, Techniques, and Procedures

Post-attack investigation revealed there may have been at least three previous terrorist attack attempts in Yemen. In the first attempt during November 1999, terrorists had planned to attack a convoy of U.S. military personnel heading to Yemen's National Center for the Removal of Land Mines. This was foiled when Yemeni security forces discovered explosives about a mile from the hotel where the Americans were staying. Suspects questioned in connection with the USS *Cole* bombing were said to have known details of the route taken by the Americans to and from the center. A second attempt allegedly targeted the Royal Hotel in Aden, where most of the 30 American servicemen were billeted. The third attempt was an intended attack on 3 January 2000 to bomb USS *The Sullivans*, a U.S. destroyer warship as it refueled in Aden.[598]

The U.S. Federal Indictment states that terrorists conducted their planning and preparations through many ruses and covert means. These included, but were not limited to, front [false] companies, false identity and travel documents, coded correspondence, and false information provided to authorities.[599]

The terrorists organized in a cellular structure for command and control. After recruitment, cell members received deliberate phases of indoctrination and training. Leaders, cadre, and supporters of this cell were focused on a particular mission and target of attacking a U.S. ship.

---

[596] Franks, 7.

[597] Department of Justice, "Al Qaeda Associates Charged in Attack on USS Cole, Attempted Attack on Another U.S. Naval Vessel," Public Relations Release #298: 05-15-03, 3; 15 May 2003; available on Http://www.usdoj.gov/opa/pr/2003/May/03_298.htm; Internet; accessed 16 February 2004.

[598] "Attack on the USS Cole," Yemen Gateway [database on-line]; available from http://www.al-bab.com/yeman/cole1.htm.

[599] Indictment S12 98 Cr. 1023, 6 and 7.

When an unexpected sinking of the terrorist bomb-boat occurred and precluded the January 2000 attack, cell members regrouped and continued to prepare for a similar mission in Aden Harbor. The sequence of planning and preparation notes a very small cell that usually compartmented knowledge among two or three individuals, and insulated more senior terrorist leaders from the specific terrorist act against the USS *Cole*.

Operational Lessons Learned

As noted in the *DOD USS Cole Commission Report*, the links between national policies and resources, and individual transiting units are the geographic Unified CINCs or military commanders-in-chief [since retitled as Combatant Commander] and their [Service] Component Commanders. First, a significant lesson learned is recognizing that transiting units do not have time or resources to focus on a series of locations while in transit. This requires these units to rely on others to support their efforts to deter, disrupt and mitigate terrorist attacks. The Component Commander has the operational war-fighting mindset for the region and is capable of controlling the resources to fight the fight and tailor specific anti-terrorism/force protection measures to protect transiting units.[600] U.S. military forces must get out of the purely defensive mode by proactively applying AT/FP techniques and assets to detect and deter terrorists. Second, an additional lesson learned is acknowledging that transfer of transiting units between and within theaters must be better coordinated. Third, a discrete operation risk management model should be adopted and utilized in AT/FP planning and execution.

Case Discussion Questions

Intelligence and Threat Warning?

What activities preceding the bombing attack might have indicated the tactical targeting of the USS *Cole* in an operational level U.S. intelligence estimate?

Security Measures in Effect?

How did U.S. force protection measures encourage the terrorists to select a U.S. Navy ship for attack?

What does the proximity of distance of the "boat bomb" detonation to the USS *Cole* suggest in force protection vulnerabilities?

Given the same bomb (IED) delivery means and scenario of the USS *Cole*, how could terrorists have increased mass casualty effects as even more devastating?

Host Nation Relationship?

How could the U.S. military unit chain of command and local Yemeni have cooperated more effectively in harbor security and post-attack investigations?

What rationale existed for choosing Aden harbor as a refueling site in the region?

---

[600] *DoD USS Cole Commission Report*, 2

Terrorist Tactics, Techniques, and Procedures?

In what other instances has al Qaeda created a vulnerability by employing innovative tactics?

Why did the terrorists use a small boat to attack the USS *Cole* in Aden harbor?

How did the terrorist group structure itself, communicate, and operate during the phases of planning and execution of the USS *Cole* bombing attack?

Assessment

International media attention spotlighted the successful terrorist maritime attack on U.S. military forces in Yemen. U.S. military forces suffered loss of life and serious wounds, and about $250 million in damage to a warship. Terrorists achieved objectives of notoriety with a worldwide audience and significant psychological trauma of a global audience through U.S. military casualties, a visibly damaged U.S. warship, and a significant escalation of maritime terrorism.

In January 2001, Usama bin Laden celebrated the bombing of USS *Cole* with a poem he recited at his son's wedding:

> A destroyer: even the brave fear its might.
> It inspires horror in the harbour [harbor] and in the open sea.
> She sails into the waves
> Flanked by arrogance, haughtiness and false power.
> To her doom she moves quickly
> A dinghy awaits her, riding the waves. [601]

U.S. military forces lost prestige when a berth for refueling considered relatively safe, was the site of a devastating attack by suicide terrorists. The Yemeni Government lost national prestige due to its inability to prevent such a terrorist attack in one of its principal harbors and seaports. The attack strained the credibility of selected Yemeni government officials with regional neighbors and commercial business associates. From an Islamic extremist perspective, the attack denounced Yemeni cooperation with U.S. military forces near the holy places of the Islamic faith.

Despite a long investigation by U.S. and Yemeni authorities there is still no conclusive proof that bin Laden specifically ordered the attack on the USS *Cole*. However, Badawi, regarded as the most senior of the *Cole* suspects who have been arrested, told his investigators that he received telephone instructions for the bombing from Mohammed Omar al-Harazi in the United Arab Emirates. Badawi said he had originally met Harazi in Afghanistan during the war.[602] Badawi indicated that Al-Harazi's tone and manner led him to believe that Al-Harazi

---

[601] "Attack on the USS Cole," Yemen Gateway [database on-line]; available from http://www.al-bab.com/yeman/cole1.htm.
[602] Ibid.

was receiving orders and financing for the attack on the USS *Cole* from bin Laden.[603] A senior Yemen government official stated that Al-Harazi was the organizer for a foiled plot to blow up the U.S. embassy in India.[604]

Figure J-11. **The USS Cole (DDG 67) Glides to Sea.**
(*Source:* U.S. Navy photo by Stacey Bynington.)

The initial damage repair estimate to the USS *Cole* (DDG 67), a modern Aegis missile equipped warship, was just under $250 million. In 2001 U.S. dollar value, this repair cost was equivalent to about one-fourth of the total construction and commissioning cost of the warship.[605] Following 14 months of repairs, the guided missile destroyer USS *Cole* (DDG 67) rejoined the U.S. Atlantic Fleet at sea in April 2002.

"We have not forgotten this nation's commitment to bring to justice all those who plot murder and orchestrate terror – no matter how long they run or how far they flee." [606]

John Ashcroft
U.S. Attorney General

Resources

Ashcroft, John. *"Remarks of Attorney General John Ashcroft, Indictment for the Bombing of the U.S.S. Cole. "* [database on-line] (Washington, D.C., 15 May 2003). Available from http://www.usdoj.gov/ag/speeches/2003/051503agremarksucccole.htm; Internet; Accessed 19 February 2004.

---

[603] "Yemen names 6 suspects in USS Cole bombing," CNN.com, World - Middle East, 13 December 2000. [database on-line]; available at http://www.cnn.com/2000/WORLD/meast/12/13/yemen.cole.ap/; Internet; accessed 26 April 2004.

[604] "Attack on the USS Cole," Yemen Gateway [database on-line]; available from http://www.al-bab.com/yeman/cole1.htm.

[605] Perl and O'Rourke, 1.

[606] John Ashcroft, "Remarks of Attorney General John Ashcroft, Indictment for the Bombing of the U.S.S. Cole, " [database on-line] (Washington, D.C., 15 May 2003); available from http://www.usdoj.gov/ag/speeches/2003/051503agremarksucccole.htm; Internet; accessed 19 February 2004.

"Attack on the USS Cole," Yemen Gateway [database on-line]. Available from http://www.al-bab.com/yeman/cole1.htm; Internet; Accessed 6 April 2004.

Franks, Tommy. "General Tommy Franks Testimony on USS Cole" [database on-line] (Washington, D.C., 25 October 2000). Available from http://www.fas.org/man/dod-101/sys/ship/docs/man-sh-ddg51-001025zd.htm. Internet. Accessed 5 April 2004.

Perl, Raphael and Ronald O'Rourke.*"Terrorist Attack on USS Cole: Background and Issues for Congress."* Congressional Research Service, The Library of Congress. Order Code RS20721, 1. 30 January 2001. Available from http://news.findlaw.com/cnn/docs/crs/coleterrattck13001.pdf; Internet; Accessed 5 April 2004.

U.S. Department of State. "Clinton Letter to Congress on U.S.S. Cole Attack," *International Information Programs, Washington File* [database on-line]. Available from
 http://usinfo.state.gov/topical/pol/terrro/00101603.htm; Internet; Accessed 1 April 2004.

U.S. Department of Defense. *DoD USS Cole Commission Report* (9 January 2001) by U.S. Army Gen. (Ret) William Crouch and U.S. Navy Adm. (Ret) Harold Gehman. open-file report, U.S. Department of Defense. 1 (Washington, D.C., 9 January 2001). Available at http://www.fas.org/irp/threat/cole.html.;Internet; Accessed 16 February 2004.

U.S. Department of Defense News Release Archive. "DoD News: Navy Announces Results of Its Investigation on USS Cole." Available from http://www.defenselink.mil/releases/2001/b011192001_bt031-01.html; Internet; Accessed 11 February 2004.

U.S. Department of Justice. "Al Qaeda Associates Charged in Attack on USS Cole, Attempted Attack on Another U.S. Naval Vessel," Public Relations Release #298: 05-15-03, 3. 15 May 2003. Available on Http://www.usdoj.gov/opa/pr/2003/May/03_298.htm; Internet; Accessed 16 February 2004.

U.S. District Court, Southern District of New York. Indictment S12 98 Cr. 1023 (KTD). United States of America, Plaintiff, vs. Jamal Ahmed Mohammed Ali Al-Badawi and Fahd Al-Quso, Defendants. Available from http://news.findlaw.com/hdocs/docs/cole/usalbadawi051503ind.pdf;
Internet; Accessed 5 April 2004.

"Yemen names 6 suspects in USS Cole bombing," CNN.com, World - Middle East, 13 December 2000. Database on-line. Available at http://www.cnn.com/2000/WORLD/meast/12/13/yemen.cole.ap/; Internet; Accessed 26 April 2004.

Page Intentionally Blank

Glossary

17 November: Revolutionary Organization 17 November based in Greece

AAIA: Aden-Abyan Islamic Army, a.k.a. Islamic Army of Aden (IAA) based in Yemen

ABB: Alex Boncayao Brigade based in the Philippines

ADCON: Administrative control, that is, exercise of authority in administration and support. See Appendix H of terrorism handbook. (JP 1-02)

ADF: Allied Democratic Forces based in Uganda and the Congo

AI: Ansar al-Islam, a.k.a. Partisans of Islam, Helpers of Islam, Supporters of Islam, Jund al-Islam, and Jaish Ansar al-Sunna based in Iraq

AIAI: Al-Ittihad al-Islami, a.k.a. Islamic Union based in Somalia

AIIB: Anti-Imperialist International Brigade, a.k.a. Japanese Red Army (JRA) based in Lebanon and Japan

Al-Badhr: Al-Badhr Mujahidin based in Pakistan

ALF: Animal Liberation Front

ALIR: Army for the Liberation of Rwanda, a.k.a. Interahamwe, Former Armed Forces of Rwanda (ex-FAR)

anarchism: A political theory holding all forms of governmental authority to be unnecessary and undesirable and advocating a society based on voluntary cooperation and free association of individuals and groups. (Webster's)

ANO: Abu Nidal Organization, a.k.a. Fatah Revolutionary Council, Arab Revolutionary Brigades, Black September, and Revolutionary Organization of Socialist Muslims based in Iraq

anti-terrorism: (AT) (JP 1-02) — Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

AOR: Area of responsibility

ASG: Abu Sayyaf Group based in the Philippines

asset (terrorist): A resource — person, group, relationship, instrument, installation, or supply — at the disposition of a terrorist organization for use in an operational or support role. Often used with a qualifying term such as suicide asset or surveillance asset. Based upon JP 1-02 asset (intelligence).

AUC: Autodefensas Unidas de Colombia, a.k.a. United Self-Defense Forces/Group of Colombia

AUM: Aum Supreme Truth, a.k.a. Aum Shinrikyo and Aleph based in Japan

backdoor: Used to describe a back way, hidden method, or other type of method of by passing normal computer security in order to obtain access to a secure area.

biological agent: (JP 1-02) — A microorganism that causes disease in personnel, plants, or animals or causes the deterioration of materiel.

biological weapon: (JP 1-02) — An item of materiel, which projects, disperses, or disseminates a biological agent including arthropod vectors.

bioregulators: (CBRN Handbook) Biochemicals that regulate bodily functions. Bioregulators that are produced by the body are termed "endogenous." Some of these same bioregulators can be chemically synthesized.

blister agents: (CBRN Handbook) Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, lungs).

blood agents: (CBRN Handbook) Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues).

BR/PCC: New Red Brigades/Communist Combatant Party, a.k.a. Brigate Rosse/Partito Comunista Combattente based in Italy

CBRNE: Chemical, biological, radiological, nuclear, and high yield explosive categories normally associated with weapons of mass destruction.

CFF: Cambodian Freedom Fighters, a.k.a. Cholana Kangtoap Serei Cheat Kampouchea based in Cambodia

chemical weapon: (JP 1-02) — Together or separately, (a) a toxic chemical and its precursors, except when intended for a purpose not prohibited under the Chemical Weapons Convention; (b) a munition or device, specifically designed to cause death or other harm through toxic properties of those chemicals specified in (a), above, which would be released as a result of the employment of such munition or device; (c) any equipment specifically designed for use directly in connection with the employment of munitions or devices specified in (b) above.

chemical agent: (CBRN Handbook) A chemical substance that is intended for use in military operations to kill, seriously injure, or incapacitate people through its physiological effects. Excluded from consideration are riot control agents, and smoke and flame materials. The agent may appear as a vapor, aerosol, or liquid; it can be either a casualty/toxic agent or an incapacitating agent.

choking agents: (CBRN Handbook) Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid. Death results from lack of oxygen; hence, the victim is "choked."

CIRA: Continuity Irish Republican Army based in Northern Ireland

conflict: (Army) — A political-military situation between peace and war, distinguished from peace by the introduction of organized political violence and from war by its reliance on political methods. It shares many of the goals and characteristics of war, including the destruction of governments and the control of territory. See FM 100-20.

COCOM: Combatant command, that is, command authority. See page 247 footnote of handbook. (JP 1-02)

consequence management: Traditionally, consequence management has been predominantly an emergency management function and included measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. The requirements of consequence management and crisis management are combined in the NRP.

CONUS: Continental United States

counter-terrorism: (CT) (JP 1-02) — Offensive measures taken to prevent, deter, and respond to terrorism.

CPP/NPA: Communist Party of the Philippines/New People's Army based in the Philippines

crisis management: Traditionally, crisis management was predominantly a law enforcement function and included measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The requirements of consequence management and crisis management are combined in the NRP.

cyber-terrorism: (FBI) — A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Defense Coordinating Officer: (DCO) The single point of contact at an incident management location for coordinating and validating the use of DOD resources. DCO works directly with the FCO or designated Federal representative, and coordinates request for assistance with the joint force commander, when a JTF is tasked to an incident response. See NRP.

Defense Information System Network: (DISN) The global, end-to-end information transfer infrastructure of DOD. It provides long haul data, voice, video, and transport networks and services needed for national defense command, control, communication, and intelligence requirements, as well as corporate defense requirements.

DSWA: Defense Special Weapons Agency

Defense Support of Civil Authorities: (DSCA) An emergent term under consideration for inclusion to the 2004 National Response Plan that incorporates the Department of Defense support to domestic emergencies, law enforcement, and other activities. A traditional overarching term is Military Assistance to Civil Authorities (MACA) which includes Military Support to Civil Authorities (MSCA) and Military Assistance to Law Enforcement (MACLEA). See NRP.

denial of service attack: (DOS) An attack designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash.

Designated Foreign Terrorist Organization: (DFTO) A political designation determined by the U.S. Department of State. Listing as a DFTO imposes legal penalties for membership, prevents travel into the U.S., and proscribes assistance and funding activities within the U.S. or by U.S. citizens. From Patterns of Global Terrorism 2001, U.S. Department of State.

DIRLAUTH: Direct liaison authorized

DFLP: Democratic Front for the Liberation of Palestine based in the Occupied Territories

DHS: Department of Homeland Security

DHKP/C: Revolutionary People's Liberation Party/Front, a.k.a. Devrimci Sol, Revolutionary Left, or Dev Sol based in Turkey

distributed denial of service attack: (DDOS) Similar to a denial of service attack, but involves the use of numerous computers to simultaneously flood the target.

Domestic Emergency Support Team: (DEST) See NRP.

dysfunctional state: Used in this circular to mean a nation or state whose declared government cannot fulfill one or more of the core functions of governance, such as defense, internal security, revenue collection, resource allocation, etc.

ELA: Revolutionary People's Struggle based in Greece

ELF: Earth Liberation Front

ELN: National Liberation Army based in Colombia

e-mail spoofing: A method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source.

Emergency Response Team: (ERT) See NRP.

ETA: Basque Fatherland and Liberty based in Spain

ETIM: Eastern Turkistan Islamic Movement based in China

FACT: Federation of Associations of Canadian Tamils, a.k.a. World Tamil Movement (WTM), World Tamil Association (WTA), Liberation Tigers of Tamil Eelam (LTTE), Ellalan Force, and Sangilian Force based in Sri Lanka

failed state: For the purposes of this circular, a dysfunctional state which also has multiple competing political factions in conflict within its borders, or has no functioning governance above the local level. This does not imply that a central government facing an insurgency is automatically a failed state. If essential functions of government continue in areas controlled by the central authority, it has not "failed."

FALN: Fuerzas Armadas de Liberacion Nacional Puertorriquena, a.k.a. Armed Forces for Puerto Rican National Liberation

FARC: Revolutionary Armed Forces of Colombia

Federal Coordinating Officer: (FCO) A Federal representative who manages Federal resource support activities related to Stafford Act disasters and emergencies; supports and is subordinate to the Principle Federal Official (PFO) when one is designated by DHS.

FEMA: Federal Emergency Management Agency. See NRP.

force protection: Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

force protection condition (FPCON): There is a graduated series of Force Protection Conditions ranging from Force Protection Conditions Normal to Force Protection Conditions Delta. There is a process by which commanders at all levels can raise or lower the Force Protection Conditions based on local conditions, specific threat information and/or guidance from higher headquarters. The four Force Protection Conditions above normal are:

Force Protection Condition ALPHA--This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of Force Protection Conditions BRAVO measures. The measures in this Force Protection Conditions must be capable of being maintained indefinitely.

Force Protection Condition BRAVO--This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this Force Protection

Conditions must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

Force Protection Condition CHARLIE--This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this Force Protection Conditions for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

Force Protection Condition DELTA--This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this Force Protection Conditions is declared as a localized condition.

FPM: Morzanist Patriotic Front based in Honduras

FPMR: Manuel Rodriquez Patriotic Front based in Chile

GIA: Armed Islamic Group based in Algeria

GICM: Moroccan Islamic Combatant Group based in Western Europe

Global Information Grid: (GIG) DOD's globally interconnected set of information capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel.

GRAPO: Grupo de Resistencia Anti-Fascista Premero de Octubre, a.k.a. First of October Antifascist Resistance Group based in Spain

GSPC: The Salafist Group for Call and Combat based in Algeria

guerrilla warfare: (JP 1-02, NATO) — Military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces. (See also unconventional warfare (UW).

GWOT: Global war on terrorism

hacker: Advanced computer users who spend a lot of time on or with computers and work hard to find vulnerabilities in IT systems.

hactivist: These are combinations of hackers and activists. They usually have a political motive for their activities, and identify that motivation by their actions, such as defacing opponents' websites with counter-information or disinformation.

HIG: Hizb-I Islami Gulbuddin based in Afghanistan and Pakistan

Homeland Security Advisory System (HSAS): The advisory system provides measures to remain vigilant, prepared, and ready to deter terrorist attacks. The following Threat

Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are suggested protective measures, recognizing that the heads of Federal departments and agencies are responsible for developing and implementing appropriate agency-specific protective measures:

- **Low Condition (Green)**. This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement: refining and exercising as appropriate preplanned Protective Measures; ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

- **Guarded Condition (Blue)**. This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: checking communications with designated emergency response or command locations; reviewing and updating emergency response procedures; and   providing the public with any information that would strengthen its ability to act appropriately.

- **Elevated Condition (Yellow)**. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement: increasing surveillance of critical locations; coordinating emergency plans as appropriate with nearby jurisdictions; assessing whether the precise characteristics of the threat require the further   refinement of preplanned Protective Measures; and implementing, as appropriate, contingency and emergency response plans.

- **High Condition (Orange)**. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; taking additional precautions at public events and possibly considering alternative venues or even cancellation; preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and restricting threatened facility access to essential personnel only.

- **Severe Condition (Red)**. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe

Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: increasing or redirecting personnel to address critical emergency needs; signing emergency response personnel and pre-positioning and mobilizing specially trained teams or resources; monitoring, redirecting, or constraining transportation systems; and closing public and government facilities.

HM: Hizb ul-Mujahidin based in Kashmir, India

HUA: Harakat ul-Ansar based in Pakistan

HUJI: Harakat ul-Jihad-I-Islami, a.k.a. Movement of Islamic Holy War based in Pakistan

HUJI-B: Harakat ul-Jihad-I-Islami/Bangladesh, a.k.a. Movement of Islamic Holy War based in Bangladesh

HUM: Harakat ul-Mujahidin, a.k.a. Movement of Holy Warriors, and Jamiat ul-Ansar (JUA) based in Pakistan

HUMINT: Human intelligence

IAA: Islamic Army of Aden, a.k.a. Aden-Abyan Islamic Army (AAIA) based in Yemen

IBDA-C: Great East Islamic Raiders – Front based in Turkey

IED: Improvised Explosive Device. Devices that have been fabricated in an improvised manner and that incorporate explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals in their design.

IG: Al-Gama'a al-Islamiyya, a.k.a. Islamic Group based in Egypt

IIPB: Islamic International Peacekeeping Brigade based in Chechnya

IMU: Islamic Movement of Uzbekistan based in Uzbekistan

incapacitating agent: (CBRN Handbook) Produce temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days, but victims usually do not require medical treatment. However, such treatment speeds recovery.

Incident Command System (ICS): A standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. The national standard for ICS is provided by NIMS.

industrial agent: (CBRN Handbook) Chemicals developed or manufactured for use in industrial operations or research by industry, government, or academia. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for use by man. Hydrogen cyanide, cyanogen chloride, phosgene, chloropicrin and many herbicides and pesticides are industrial chemicals that also can be chemical agents.

INLA: Irish National Liberation Army based in Northern Ireland

INRP: Initial National Response Plan. As the time of this handbook publication, is a final draft document that consolidates several Federal-level incident management and emergency response plans into a national framework for domestic incident management.

insurgency: (JP 1-02, NATO) — An organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict.

international: of, relating to, or affecting two or more nations (Webster's). For our purposes, affecting two or more nations.

IP address spoofing: A method that creates Transmission Control Protocol/Internet Protocol (TCP/IP) packets using somebody else's IP address

IRA: Irish Republican Army based in Northern Ireland

IMU: Islamic Movement of Uzbekistan

JEM: Jaish-e-Mohammed, a.k.a. Army of Mohammed based in Pakistan

JI: Jemaah Islamiya based in Malaysia and Singapore

Joint Field Office: (JFO) See National Response Plan.

JRA: Japanese Red Army, a.k.a. Anti-Imperialist International Brigade (AIIB) based in Lebanon and Japan

JUA: Jamiat ul-Ansar, a.k.a. Harakat ul-Mujahidin (HUM), and Movement of Holy Warriors

JUD: Jamaat ud-Dawa, a.k.a. Lashkar-e-Tayyiba, and Army of the Righteous (LT) based in Pakistan

JUM: Jamiat ul-Mujahidin based in Kashmir, India

KADEK: Kurdistan Freedom and Democracy Congress, a.k.a. Kongra-Gel (KGK), Kurdistan Workers' Party (PKK), and Freedom and Democracy Congress of Kurdistan based in Turkey

keylogger: A software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard.

KGK: Kongra-Gel, a.k.a. Kurdistan Workers' Party (PKK), Kurdistan Freedom and Democracy Congress (KADEK), and Freedom and Democracy Congress of Kurdistan based in Turkey

KMM: Kumpulan Mujahidin Malaysia based in Malaysia

LFA: Lead Federal Agency. See NRP.

LJ: Lashkar I Jhangvi, a.k.a. Army of Jhangvi based in Pakistan

logic bomb: A program routine that destroys data by reformatting the hard disk or randomly inserting garbage into data files.

LRA: Lord's Resistance Army based in Uganda

LT: Lashkar-e-Tayyiba, a.k.a. Army of the Righteous and Jamaat ud-Dawa (JUD) based in Pakistan

LTTE: Liberation Tigers of Tamil Eelam, a.k.a. World Tamil Association (WTA), World Tamil Movement (WTM), Federation of Associations of Canadian Tamils (FACT), Ellalan Force, and Sangilian Force based in Sri Lanka

LVF: Loyalist Volunteer Force based in Northern Ireland

MAGO: Muslims Against Global Oppression, a.k.a. Qibla and People Against Gangsterism and Drugs (PAGAD), and Muslims Against Illegitimate Leaders (MAIL) based in South Africa

MAIL: Muslims Against Illegitimate Leaders, a.k.a. Muslims Against Global Oppression (MAGO), and Qibla and People Against Gangsterism and Drugs (PAGAD) based in South Africa

MCC: The Maoist Communist Center, a.k.a. Naxalites and Maoist Communist Center of India (MCCI) based in India

MCCI: Maoist Communist Center of India, a.k.a. The Maoist Communist Center (MCC) and Naxalites based in India

MEK: Mujahidin-e Khalq Organization, a.k.a. Holy Warriors of the People, National Liberation Army of Iran (NLA), People's Mujahidin of Iran (PMOI), National Council of Resistance (NCR), National Council of Resistance of Iran (NCRI), and Muslim Iranian Student's Society based in Iraq

millenarian: Apocalyptic; forecasting the ultimate destiny of the world; foreboding imminent disaster or final doom; wildly unrestrained; ultimately decisive. (Merriam –Webster's)

MRTA: Tupac Amaru Revolutionary Movement based in Peru

narco-terrorism: (JP 3-07.4) Terrorism conducted to further the aims of drug traffickers. It may include assassinations, extortion, hijackings, bombings, and kidnappings directed against judges, prosecutors, elected officials, or law enforcement agents, and general disruption of a legitimate government to divert attention from drug operations.

nation: A community of people composed of one or more nationalities and possessing a more or less defined territory and government or a territorial division containing a body of people of one or more nationalities and usually characterized by relatively large size and independent status.

nation-state: A form of political organization under which a relatively homogeneous people inhabits a sovereign state; especially a state containing one as opposed to several nationalities.

NCR: National Council of Resistance, a.k.a. National Liberation Army of Iran (NLA), Mujahidin-e Khalq Organization (MEK), Holy Warriors of the People, People's Mujahidin of Iran (PMOI), National Council of Resistance of Iran (NCRI), and Muslim Iranian Student's Society based in Iraq

NCRI: National Council of Resistance of Iran, a.k.a. National Liberation Army of Iran (NLA), Mujahidin-e Khalq Organization (MEK), Holy Warriors of the People, People's Mujahidin of Iran (PMOI), National Council of Resistance (NCR), and Muslim Iranian Student's Society based in Iraq

nerve agents: (CBRN Handbook) Substances that interfere with the central nervous system. Exposure is primarily through contact with the liquid (skin and eyes) and secondarily through inhalation of the vapor. Three distinct symptoms associated with nerve agents are: pin-point pupils, an extreme headache, and severe tightness in the chest.

National Incident Management System: (NIMS). See *National Incident Management System* published by the Department of Homeland Security, 1 March 2004. The NIMS represents a core set of doctrine, concepts, principles, technology and organizational processes to enable effective, efficient, and collaborative incident management. Nationwide context is an all-hazards, all jurisdictional levels, and multi-disciplines approach to incident management.

NIPR: Revolutionary Proletarian Initiative Nuclei based in Italy

NLA: National Liberation Army of Iran, a.k.a. Mujahidin-e Khalq Organization (MEK), Holy Warriors of the People, People's Mujahidin of Iran (PMOI), National Council of Resistance (NCR), National Council of Resistance of Iran (NCRI), and Muslim Iranian Student's Society based in Iraq

NPA: New People's Army based in the Philippines

National Response Plan (NRP): See NRP (Final Draft as of 30 June 2004).

NTA: Anti-Imperialist Territorial Nuclei based in Italy

nuclear weapon: (JP 1-02) — A complete assembly (i.e., implosion type, gun type, or thermonuclear type), in its intended ultimate configuration which, upon completion of the prescribed arming, fusing, and firing sequence, is capable of producing the intended nuclear reaction and release of energy.

OPCON: Operational control, that is, transferable command authority. See Appendix H of terrorism handbook. (JP 1-02).

operations security: (OPSEC) A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

OV: Orange Volunteers based in Northern Ireland

PAGAD: Qibla and People Against Gangsterism and Drugs, a.k.a. Muslims Against Global Oppression (MAGO), and Muslims Against Illegitimate Leaders (MAIL) based in South Africa

Pathogen: (CBRN Handbook) Any organism (usually living) capable of producing serious disease or death, such as bacteria, fungi, and viruses

PFLP: The Popular Front for the Liberation of Palestine based in Syria

PFLP-GC: The Popular Front for the Liberation of Palestine – General Command based in Syria

physical security: That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub1-02)

PIJ: The Palestine Islamic Jihad based in Syria

PIRA: Provisional Irish Republican Army based in Northern Ireland

PKK: Kurdistan Workers' Party, a.k.a. Kongra-Gel (KGK), Kurdistan Freedom and Democracy Congress (KADEK), and Freedom and Democracy Congress of Kurdistan based in Turkey

PLF: Palestine Liberation Front based in Iraq

PMOI: People's Mujahidin of Iran, a.k.a. National Liberation Army of Iran (NLA), Mujahidin-e Khalq Organization (MEK), Holy Warriors of the People, National Council of Resistance (NCR), National Council of Resistance of Iran (NCRI), and Muslim Iranian Student's Society based in Iraq

Principle Federal Official: (PFO) Senior representative of Secretary of Homeland Security and lead Federal official on-scene to coordinate Federal domestic incidents management and resource allocation on-scene. See NRP.

PWG: Peoples War Group, a.k.a. Peoples War and Naxalites based in India

Radiological Dispersal Device: (RDD) (CBRN Handbook) A device (weapon or equipment), other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material.

Radiological Emitting Device: (RED) A device designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material. RED dissemination techniques can include intense, short duration exposure or progressive, long term exposure to radiation.

radiological operation: (JP 1-02) — The employment of radioactive materials or radiation producing devices to cause casualties or restrict the use of terrain. It includes the intentional employment of fallout from nuclear weapons.

RIRA: Real IRA, a.k.a. True IRA based in Northern Ireland

RHD: Red Hand Defenders based in Northern Ireland

RN: Revolutionary Nuclei based in Greece

RSRSBCM: Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs based in Chechnya

RUF: Revolutionary United Front based in Sierra Leone

setback: Distance between outer perimeter and nearest point of buildings or structures within. Generally referred to in terms of explosive blast mitigation.

SL: Sendero Luminoso, a.k.a. Shining Path based in Peru

sniffer: A program and/or device that monitors data traveling over a network.

SPIR: Special Purpose Islamic Regiment based in Chechnya

SSP: Sipah-I-Sahaba/Pakistan based in Pakistan

state: A politically organized body of people usually occupying a definite territory; especially one that is sovereign.

steganography: The process of hiding information by embedding messages within other, seemingly harmless messages. The process works by replacing bits of useless or unused

data in regular computer files (such as graphics, sound, text) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

TACON: Tactical control, that is, command authority with detailed limitations and responsibilities inherent to operational control. See Appendix H of terrroism handbook. (JP 1-02).

TCG: The Tunisian Combatant Group, a.k.a. The Tunisian Islamic Fighting Group or Jama'a Combattante Tunisienne based in Tunisia

terror tactics: Given that the Army defines tactics as **"**the art and science of employing available means to win battles and engagements," then terror tactics should be considered "the art and science of employing violence, terror and intimidation to inculcate fear in the pursuit of political, religious, or ideological goals."

terrorism: (JP 1-02) — The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

terrorist: (JP 1-02) — An individual who uses violence, terror, and intimidation to achieve a result.

terrorist goals: The term *goals* will refer to the strategic end or end state that the terrorist objectives are intended to obtain. Terrorist organization goals equate to the strategic level of war as described in FM 101-5-1.

terrorist group: Any group practicing, or that has significant subgroups that practice, international terrorism (U.S. Dept of State)

terrorist objectives: The standard definition of *objective* is – "The clearly defined, decisive, and attainable aims which every military operation should be directed towards" (JP 1-02). For the purposes of this work, terrorist objectives will refer to the intended outcome or result of one or a series of terrorist operations or actions. It is analogous to the tactical or operational levels of war as described in FM 101-5-1.

toxic chemical agent: (CBRN Handbook) Produce incapacitation, serious injury, or death. They can be used to incapacitate or kill victims. These agents are the choking, blister, nerve, and blood agents.

toxin agent: (JP 1-02) — A poison formed as a specific secretion product in the metabolism of a vegetable or animal organism, as distinguished from inorganic poisons. Such poisons can also be manufactured by synthetic processes.

transnational: Extending or going beyond national boundaries (Webster's). In this context, not limited to or centered within a single nation.

trojan horse: A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed performs a function in the background such as

allowing other users to have access to your computer or sending information from your computer to other computers.

virus: A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program.

UDA/UFF: Ulster Defense Association/Ulster Freedom Fighters based in Northern Ireland

underground: A covert unconventional warfare organization established to operate in areas denied to the guerrilla forces or conduct operations not suitable for guerrilla forces.

unified command: As a term in the Federal application of the Incident Command System (ICS), defines agencies working together through their designated Incident Commanders at a single Incident Command Post (ICP) to establish a common set of objectives and strategies, and a single Incident Action Plan. This is NOT "unified command" as defined by the Department of Defense.

UVP: Ulster Defense Force based in Northern Ireland

UXO: Unexploded ordnance

VBIED: Vehicle borne improvised explosive device

WOT: War on terrorism

WTA: World Tamil Association, a.k.a. Liberation Tigers of Tamil Eelam (LTTE), World Tamil Movement (WTM), Federation of Associations of Canadian Tamils (FACT), Ellalan Force, and Sangilian Force based in Sri Lanka

WTM: World Tamil Movement, a.k.a. World Tamil Association (WTA), Liberation Tigers of Tamil Eelam (LTTE), Federation of Associations of Canadian Tamils (FACT), Ellalan Force, and Sangilian Force based in Sri Lanka

WCOTC: World Church of the Creator

WEG: Worldwide Equipment Guide. A document produced by the TRADOC ADCSINT – Threats that provides the basic characteristics of selected equipment and weapons systems readily available for use by the OPFOR.

WMD: (JP 1-02)   — Weapons of Mass Destruction. Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

WMD-CST: Weapons of Mass Destruction – Civil Support Team

WMD/E: Weapons of mass destruction or effect is an emergent term referenced in the 2004 U.S. National Military Strategy to address a broader range of adversary capabilities with potentially devastating results.

worm: A destructive software program containing code capable of gaining access to computers or networks and once within the computer or network causing that computer or network harm by deleting, modifying, distributing, or otherwise manipulating the data.

zombie: A computer or server that has been basically hijacked using some form of malicious software to help a hacker perform a Distributed Denial Of Service attack (DDOS).

Selected Bibliography

ABCNews.com, 18 October 2000. Available from http://www.abcnews.go.com/ sections/ world/DailyNews/cole001018b.html; Internet; Accessed 9 January 2003.

"Abu Nidal." *Encyclopedia of the Orient*. Available from http://i-cias.com/e.o/abu_nidal.htm; Internet; Accessed 24 February 2004.

"Abu Nidal Organization." *Terrorism Questions and Answers.* Available from http://cfrterrorism.org/groups/abunidal.html. Internet; Accessed 24 February 2004.

"Abu Nidal Organization (ANO)." *FAS Intelligence Resource Program.* Available from http://www.fas.org/irp/world/para/ano.htm; Internet; Accessed 24 February 2004.

"April 1983 US Embassy bombing." Available from http://encyclopedia.the freedictionary.com/April%2011983%20US%20Embassy%20bombing; Internet; Accessed 1 July 2004

Albright, David. "Al Qaeda's Nuclear Program: Through the Window of Seized Documents." *Policy Forum Online* 47 (6 November 2002): 1-12. Available from http://www.nautilus.org/fora/Special-Policy-Forum/47_Albright.html; Internet; Accessed 13 February 2003.

Anderson, Sean K., and Stephen Sloan. *Historical Dictionary of Terrorism.* Lanham, MD: Scarecrow Press, Inc, 2002.

AR 190-52. *Countering Terrorism and Other Major Disruptions on Military Installations*. 1978.

Aras, Djanguir. *Militant 2000: World Handbook on Non-governmental Militarized Structures*. Baku: Center for Low Intensity Conflict Studies, 2000.

Army War College, *How The Army Runs; A Senior Leader Reference Handbook 2003-2004.* Carlisle, PA: U.S. Army War College, Department of Command, Leadership, and Management, 23 September 2003. Available at http://carlisle-www.army.mil/usawc/dclm/linkedtextchapters.htm; Internet; Accessed 31 December 2003.

Arquilla, John and David Ronfeldt, ed. *Networks and Netwars*. Santa Monica: RAND, 2001.

Ashcroft, John. *"Remarks of Attorney General John Ashcroft, Indictment for the Bombing of the U.S.S. Cole. "*Washington, D.C., 15 May 2003. Available from http://www.usdoj.gov/ag/speeches/2003/051503agremarksucccole.htm; Internet; Accessed 19 February 2004.

Associated Press Newswires. 12 February 2002. Available from http://www. Stop eco violence.org/pdfs/2_12_02.pdf; Internet; Accessed 17 January 2003.

"Attack on the USS Cole." Yemen Gateway. Available from http://www.al-bab.com/yeman/cole1.htm; Internet; Accessed 6 April 2004.

Axtman, Kris. "The Terror Threat At Home, Often Overlooked." *Christian Science Monitor,* 29 December 2003. Available at http://ebird.afis.osd.mil/ebfiles/s20031229244982.html; Internet; Accessed 29 December 2003.

"2002 Bali Terrorist Bombing." *Wikipedia*, 2004 ed., s.v. Available from http://en.wikipedia.org/w/wiki.phtml?title=2002_Bali_terrorist_bombing&printable=yes; Internet; Accessed 17 March 2004.

The Basics of Terrorism: Parts 1-6. The Terrorism Research Center, 1997. Available from http://www.terrorism.com/terrorism/bpart1.html through /bpart6.html; Internet; Accessed 29 August 2002.

BBC News, 21 December 1998. Available from http://news.bbc.co.uk/1/hi/special _report/1998/12/98/lockerbie/235632.stm; Internet; Accessed 12 December 2002.

Beyler, Clara. "Messengers of Death – Female Suicide Bombers." *International Policy Institute for Counterterrorism* (12 February 2003): 3. Available from http://www.ict.org.il/articles/articledet.cfm?articleid=470; Internet; Accessed 18 March 2004.

_____. "Female Suicide Bombers – An Update." *International Policy Institute for Counterterrorism* 7 March 2004: 1. Available from http://www.ict.org.il/articles/articledet.cfm?articleid=508; Internet; Accessed 31 March 2004.

Billingslea, William. "Illicit Cigarette Trafficking and the Funding of Terrorism." *The Police Chief*, February 2004. 49-54.

Blythe, Will. "A Weatherman in Autumn." *Newsweek: Arts & Opinion*, 12 June 2003. Available from http://msnbc.msn.com/id/3069267/; Internet; Accessed 12 February 2004.

Bolkcom, Christopher, Bartholomew Elias, and Andrew Feickert. *Homeland Security: Protecting Airliners from Terrorist Missiles*. Washington, D.C.: Congressional Research Service Report for Congress, November 3, 2003. Available from http://www.fas.org/irp/crs/RL31741.pdf; Internet; Accessed 1 April 2004.

Bowman, Steve. *Homeland Security: The Department of Defense's Role.* Congressional Research Service Report for Congress, Order Code RL 31615, 7, 14 May 2003.

_____. *Weapons of Mass Destruction: The Terrorist Threat.* Washington, D.C.: Congressional Research Service Report for Congress, 7 March, 2002. Available from http://www.fas.org/irp/crs/RL31332.pdf; Internet; Accessed 23 December 2002.

Bryan, Major General James D. *See* U.S. Congress.

Burghardt, Tom. "Leaderless Resistance and the Oklahoma City Bombing." BACORR: Bay Area Coalition for Our Reproductive Rights. Available from http://nwcitizen.com/publicgood/reports/leadless.htm; Internet; Accessed 10 February 2004.

Burke, Jason. "You Have to Kill in the Name of Allah until You are Killed." *Guardian Unlimited* Observer Special Report, 27 January 2002: 1-6. Available from http://www.observer.co.uk/islam/story/0,1442,640288,00.html; Internet; Accessed 15 January 2003.

Buse, Margaret. "Non-State Actors and Their Significance." *Journal of Mine Action* (December 2002): 1-9. Available from http://maic.jmu.edu/journal/5.3/features/_maggie_buse_nsa/maggie_buse.htm; Internet; accessed 13 December 2002.

"CAMERA ALERT: CBS' 60 Minutes Exposes. "The Arafat Papers." Available from http://www.camera.org/index.asp?x_article=289&x_context=3; Internet; Accessed 2 February 2004.

Canadian Security Intelligence Service. "Report 2000/05 Biological Weapons Proliferation." *Perspectives* (9 June 2000): 1-8. Available from http://www.csis-scrs.gc.ca/eng/_miscdocs/200005_e.html; Internet; Accessed 6 February 2003.

Carr, Caleb. *The Lessons of Terror: A History of Warfare Against Civilians: Why it has Always Failed and Why it will Fail Again.* New York: Random House, 2002.

Carr, Caleb. "TIME.com Interview with Calib Carr." 1 February 2002. Available at http://www.time.com/time/2002/carr/interview.html; Internet; Accessed 31 August 2004.

CBS News.com, 21 January 2003. Available from http://www.cbsnews.com/stories/2003/01/21/attack/main537258.shtml; Internet; Accessed 10 February 2003.

CBS News.com. "Evidence Points to Yemen Terror Attack." Available from http://www.cbsnews.com/stories/2002/10/06/world/main524488.shtml; Internet; Accessed 21 January 2004.

Central Intelligence Agency. Director of Central Intelligence. *Cyber Threat Trends and U.S. Network Security.*` Statement for the Record for the Joint Economic Committee by Lawrence K. Gershwin, National Intelligence Officer for Science and Technology. (Washington, D.C., 21 June 2001), 1. Available from http://www.cia.gov/cia/public_affairs/speeches/2001/gershwin_speech_06222001.html; Internet; Accessed 14 April 2004.

Chalk, Peter. "Threats to the Maritime Environment: Piracy and Terrorism." RAND Stakeholder Consultation briefing presented at Ispra, Italy 28-30 October 2002. Available from http://www.rand.org/randeurope/news/seacurity/piracyterrorism.chalk. pdf; Internet; Accessed 4 April 2004.

"'Chemistry 101': The Make-up and Importance of Radioisotopes." *Introduction to Radiological Terrorism,* 1. Available from http://www.nti.org/h_learnmore/radtutorial/chapter01_03.html; Internet; Accessed 19 May 2004.

Chester, Steven A. *See* U.S. Department of Defense.

Chetak's Explosive Pages. Chetak's Website, 2002. Available from http://www.geocities. com/chetak74/explosives.html; Internet; Accessed 11 December 2002.

"Chinese Satellite TV Hijacked by Falun Gong Cult." *People's Daily Online*, 9 July 2002. Available from http://english.peopledaily.com.cn/200207/08/eng20020708_99347.shtml; Internet; Accessed 27 Nov 2002.

CJCS CONPLAN 0500-98. *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive Situation.* 11 February 2002.

CJCSI 3125.01. *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Situation.* 3 August 2001.

Clark, C.J. *Mine/UXO Assessment: Former Yugoslav Republic of Macedonia.* New York: United Nations Mine Action Coordination Center, 8 October 2001. Available from http://www.mineaction.org/sp/mine_awareness/_refdocs.cfm?doc_ID=707; Internet; Accessed 13 December 2002.

CNN.com, 10 October 1995. Available from http://www.cnn.com/US/9510/amtrak/10-10/; Internet; Accessed 15 January 2003.

CNN.com International, "Fuel rod parts missing from nuclear plant," 22 April 2004. Available from http://edition.cnn.com/2004/US/Northeast/04/21/nuclear.fuel.missing.ap/index.html; Internet; Accessed 22 April 2004.

CNN.com LAW CENTER, 10 August 2004. "Terry Nichols Gets Life, No Parole." Available on http://www.cnn.com/2004/LAW/08/09/Nichols.sentence.ap/; Internet; Accessed 25 August 2004.

CNN.com./WORLD, 22 November 2002. "Fishing Boat Explodes Near Israeli Vessel." Available from http://www.cnn.com/2002/WORLD/meast/11/22/mideast/; Internet; Accessed 21 January 2004.

CNN.com, World - Middle East, 13 December 2000. "Yemen Names 6 Suspects in USS *Cole* Bombing." Available at http://www.cnn.com/2000/WORLD/meast/12/13/yemen.cole.ap/; Internet; Accessed 26 April 2004.

CNS News.com, 3 December 2002. Available from http://www.cnsnews.com/ ForeignBureaus/archive/200212/FOR20021203a.html; Internet; Accessed 19 March 2004.

Cohen, William S. *See* U.S. Department of Defense.

Coleman, Kevin. "Cyber Terrorism," *Directions Magazine,* 10 October 2003. Available from http://www.directionsmag.com/article.php?article_id=432; Internet; Accessed 15 March 2004.

Colonel James "Nick" Rowe. Psychological Operations Website, n.d. Available from http://www.psywarrior.com/ rowe.html; Internet; Accessed 7 January 2003.

Committee on the Judiciary Subcommittee on Crime. Opening Statement by Louis J. Freech, Director, Federal Bureau of Investigation Before the Committee on the Judiciary Subcommittee on Crime. 104th Congress, 3 May 1995. Available from http://www.lectlaw.com/files/cur13.htm; Internet; Accessed 5 March 2004.

Conventional Terrorist Weapons. New York: United Nations Office for Drug Control and Crime Prevention, 2002. Available from http://www.undcp.org/odccp/terrorism _weapons_conventional.html; Internet; Accessed 12 November 2002.

Corpus, Victor N. "The Invisible Army." Briefing presented at Fort Leavenworth, KS, 5 November 2002. TRADOC ADCSINT-Threats Files, Fort Leavenworth, KS.

Crenshaw, Martha. "The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice." In *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, rev. ed., edited by Walter Reich. Washington: Woodrow Wilson Center Press, 1998.

Cyber-Terrorism. Statement by Major General James D. Bryan, U.S. Army Commander, Joint task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency. Washington, D.C., 24 July 2003, 5. Available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; Accessed 6 April 2004.

DA Pamphlet 550-104. *Human Factors Considerations of Undergrounds in Insurgencies,* September 1966.

"Defense Information System Network." Defense Information Systems Agency, Network Services [Website on line, n.d.]. Available from http://www.disa.mil/ns/gig.html; Internet; Accessed 7 April 2004.

Defense Threat Reduction Agency. *Domestic WMD Incident Management Legal Deskbook*, 3-12 and 3-13, December 2003. Available at http://biotech.law.lsu.edu/blaw/DOD/manual; Internet; Accessed 23 April 2004.

Director of Central Intelligence, DCI Weapons Intelligence, Nonproliferation, and Arms Control Center. *Unclassified Report to Congress on the Acquisition of Technology Reacting to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2003*, 11. Available from http://www.cia.gov/cia/reports/721_reports/pdfs/jan_jun2003.pdf; Internet; Accessed 19 may 2004.

"Dirty Bombs: Response to a Threat." FAS Public Interest Report, *The Journal of the Federation of American Scientists* 55 no. 2 (March/April 2002), 1-11. Available from http://ww.fas.org/faspir/2002/v55n2/dirtybomb.htm; Internet; Accessed 15 April 2004.

Dobson, Christopher, and Ronald Payne. *The Terrorist: Their Weapons, Leaders, and Tactics.* New York: Facts on File, Inc, Revised Edition, 1982.

DOD Directive 3025.1, *Military Support to Civil Authorities* (MSCA), 15 January 1993.

DOD Directive 3025.12, *Military Assistance for Civil Disturbances* (MACDIS), 4 February 1994.

DOD Directive 3025.15, *Military Assistance to Civil Authorities*, 18 February 1997.

Dolinar, Lou. "Cell Phones Jury-rigged to Detonate Bombs." *Newsday.com*, 15 March 2004. Available from http://www.newsday.com/news/nationworld/ny-wocell153708827mar15,0,1644248.story?coll=ny-nationworld-headlines; Internet; Accessed 15 March 2004.

"Economic Effects." *Introduction to Radiological Terrorism,* 1. Available from http://www.nti.org/h_learnmore/radtutorial/chapter02_02.html; Internet; Accessed 19 May 2004.

Ehrenfeld, Rachael. *IRA + PLO + Terror.* Journal on-line. American Center for Democracy (ACD), 21 August 2002. Available from http://public-integrity.org/publications21.htm; Internet; Accessed 13 February 2004.

"Eligible Receiver." *Global Security.org*, 9 June 2002. Available from http://www.globalsecurity.org/military/ops/eligible-receiver.htm; Internet; Accessed 24 June 2004.

Ellis, John. "In My Humble Opinion: Genomics is the Most Economic, Political, and Ethical Issue Facing Mankind." *Fast Company*, November 1999. Available from http://www.fastcompany.com/online/29/jellis.html; Internet; Accessed 26 February 2004.

"Fact Sheet on the Accident at the Chernobyl Nuclear Power Plant." U.S. Nuclear Regulatory Commission, 1. Available at http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fschernobyl.html; Internet; Accessed 1 July 2004.

"Fact Sheet on the Accident at Three Mile Island." U.S. Nuclear Regulatory Commission, 1 to 5. Available at http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle,html; Internet; Accessed 1 July 2004.

Falkenrath, Richard A. "Problems of Preparedness: US Readiness for a Domestic Terror Attack." *International Security* 25, no. 4 (Spring 2001): 147-186.

"False Calls on Casualties Upset Camp Pendleton Spouses." *Mustang Daily Online News*, 11 April 2003. Available from http://www.mustangdaily.calpoly.edu/archive/20030411/print.php?story=inat; Internet; Accessed 13 August 2004.

Fischer, Lynn F. *The Threat Of Domestic Terrorism.* The Terrorism Research Center, 2002. Available from http://www.terrorism.com/terrorism/DomesticThreat.shtml; Internet; Accessed 10 September 2002.

FM 3-06. *Urban Operations*. June 2003.

FM 3-23.30. *Grenades and Pyrotechnic Signals*. September 2000.

FM 5-25. *Explosives and Demolitions*. March 1986.

FM 7-100. *Opposing Force Doctrinal Framework and Strategy*. May 2003.

FM 20-32. *Countermine Operations*. October 2002.

FM 100-20. *Military Operations in Low Intensity Conflict*. December 1990.

FM 100-37. *Terrorism Counteraction*. July 1987.

FM 101-5-1. *Operational Terms and Graphics*. 30 September 1997.

Ford, Franklin L. *Political Murder: From Tyrannicide to Terrorism.* Cambridge: Harvard University Press, 1985.

Frances, Sabil. "Uniqueness of LTTE's Suicide Bombers." *Institute of Peace and Conflict Studies*, Article no. 321 (4 February 2000): 1. Available from http://www.ipcs.org; Internet; Accessed 7 September 2002.

Franks, Tommy. "General Tommy Franks Testimony on USS Cole." Washington, D.C., 25 October 2000. Available from http://www.fas.org/man/dod-101/sys/ship/docs/man-sh-ddg51-001025zd.htm; Internet; Accessed 5 April 2004.

Freeh, Louis. *See* Committee on the Subcommittee on Crime.

"French Tanker Explosion Confirmed as Terror Attack." Available from http://www.ict.org.il/spotlight/det.cfm?id=837; Internet; Accessed 21 January 2004.

Freund, Charles Paul. "Old School Osama: What We Found While Looking for Bin Laden." *Reason Online* 12 September 2002: 1-7. Available from http://reason.com/_hod/cpf091202.shtml; Internet; Accessed 12 September 2002.

Frittelli, John F. Port and Maritime Security: Background and Issues for Congress. Washington, D.C.: Congressional Research Service Report for Congress, December 5, 2003. Available from http://www.usembassy.at/en/download/pdf/port_sec.pdf; Internet; Accessed 5 April 2004.

"From Push to Shove." *Southern Poverty Law Center Intelligence Report,* no. 107 (Fall 2002): 1-18. Available from http://www.splcenter.org/intelligenceproject/ip-index.html; Internet; Accessed 17 January 2003.

Fuller, Fred L. "New Order Threat Analysis: A Literature Survey." *Marine Corps Gazette*, 81 (April 1997): 46-48.

Garamone, Jim. *See* U.S. Department of Defense.

Gellman, Bartom. "Cyber-Attacks by Al Qaeda Feared," *Washingtonpost.com,* 27 June 2002. Available from http://www.wahsingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; Accessed 12 April 2004.

"Global Information Grid." Defense Information Systems Agency, Network Services Website on line, n.d. Available from http://www.disa.mil/ns/gig.html; Internet; Accessed 7 April 2004.

Gorin, Stuart. "Timothy McVeigh Executed for Oklahoma City Bombing." Washington File Staff Writer; U.S. Department of State International Information Programs. 11 June 2001. Available from http://usinfo.state.gov/topical/pol/terrro/01061101.htm; Internet; Accessed 16 February 2004.

Gray, Colin S. "Thinking Asymmetrically in Times of Terror." *Parameters* (Spring, 2002): 5-14.

Greenberg, Maurice R., Chair; William F. Wechsler, and Lee S. Wolosky, Project Co-Directors. *Terrorist Financing: Report of an Independent Task Force Sponsored by the Council on Foreign Relations.* New York: Publication Office, Council on Foreign Relations, 25 November 2002.

Gresh, Alain. "The unsolved mystery of a Saudi bomb attack." *Le Monde diplomatique.* September 1997, 2. Available from http://mondediplo.com/1997/09/saudi; Internet; Accessed 19 February 2004.

Grigg, William Norman. "'Respectable' Terrorists." *The New American,* 19 November 2001. Available from http://www.the newamerican.com/tna/2001/11-19-2001/vol17no24_terrorists.htm; Internet; Accessed 12 February 2004.

Gunaratna, Rohan. "Suicide Terrorism: A Global Threat." *Jane's Intelligence Review* (20 October 2000): 1-7. Available from http://www.janes.com/security/international _security/news/usscole/jir001020_1_n.shtml; Internet; Accessed 7 September 2002.

_____. "Suicide Terrorism in Sri Lanka and India." In *Countering Suicide Terrorism.* Herzilya, Israel: The International Policy Institute for Counter Terrorism, The Interdisciplinary Center, 2002.

Harmon, Christopher C. *Terrorism Today.* London: Frank Cass Publishers, 2000;Reprint, Portland: Frank Cass Publishers, 2001.

Hellman, Christopher, and Reyko Huang. *List of Known Terrorist Organizations.* Washington: Center for Defense Information Terrorism Project, 2001. Available from http://www.cdi.org/terrorism/terrorist-groups-pr.cfm; Internet; Accessed 24 October 2002.

Hendershot, Harold M. "CyberCrime 2003 – Terrorists' Activity in Cyberspace." [Briefing slides from the Cyber Division] Federal Bureau of Investigation, Washington, D.C. Available from http://www.4law.co.il/L373.pdf; Internet; Accessed 6 April 2004.

Henderson, Harry. *Terrorism.* New York: Facts on File, 2001.

Hettena, Seth . "Earth Liberation Front Claims Responsibility for San Diego Arson." *The Mercury News*, 18 August 2003. Available from http://www.mercurynews.com/mld/mercurynews/news/local/6562462.htm; Internet; Accessed 17 March 2004.

"History of Radiological Terrorism." *Introduction to Radiological Terrorism, 1 to* 3. Available from http://www.nti.org/h_learnmore/radtutorial/chapter03_01.html; Internet; Accessed 19 May 2004.

"History of the United Nations and Chernobyl." The United Nations and Chernobyl, 1. Available at http://www.un.org/ha/Chernobyl; Internet; Accessed 1 July 2004

Hoffman, Bruce. "All You Need Is Love: How the Terrorists Stopped Terrorism." *Atlantic Monthly* December 2001: 1-6. Available from http://www.theatlantic.com/issues/ 2001/12/hoffman.htm; Internet; Accessed 21 October 2002.

_____. *Inside Terrorism.* New York: Columbia University Press, 1998.

Homer-Dixon, Thomas. "The Rise of Complex Terrorism." *Foreign Policy Magazine* 1, 6, and 7, January-Febraury 2002; available from http:// www.foreighnpolicy.com/story/cms.php?story_id=170; Internet; accessed 26 August 2004.

Huntington, Samuel."The Clash of Civilizations." *Foreign Affairs* (Summer 1993): 1-29. Available from http://www.lander.edu/atannenbaum/Tannenbaum%20courses% 20folder/POLS%20103%20World%20Politics/103_huntington_clash_of_civilizations_full_text.htm#I.%2 0THE%20NEXT%20PATTERN%20OF%20CONFLICT; Internet; Accessed 6 December 2002.

Illegal Incidents Report. Washington: Foundation for Biomedical Research, 2002. Available from http://www.fbresearch.org/animal-activism/eventsummary.xls; Internet; Accessed 4 December 2002.

Improvised Explosives, vol. I*, version 2.0. N.p., 15 May 1990. Available from http://www. logicsouth.com/~lcoble/password/firearms.html; Internet; Accessed 11 December 2002.

Improvised Explosives. N.p., n.d. Available from http://members.odinsrage.com/ white88/ 18_ImprovisedExplosives.htm; Internet; Accessed 11 December 2002.

Improvised Explosive Devices. Salem: Oregon State Police Website, 2002. Available from http://www.osp.state.or.us/html/improvised_explosives.html; Internet; Accessed 11 December 2002.

International Encyclopedia of Terrorism, 1997 ed., s.v. "The Media and International Terrorism."

International Herald Tribune, 25 March 2004. Available from http://iht.com/articles/511745.html; Internet; Accessed 26 March 2004.

Italiansrus.com. Di Meglio, Francesco. "Italian Terrorists Generate Fear in Europe." Available from http://www.italianrus.com/articles/ourpaesani/redbrigade.htm; Internet; Accessed 25 February 2004.

Jarboe, James. *See* U.S. Congress.

Jenkins, Brian. *See* National Commission on Terrorist Attacks Upon the United States.

Joint Chiefs of Staff, *National Military Strategy of the United States of America*, 1, May 2004.

Joint Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 12 April 2001, as amended through 9 June 2004.

Joint Pub 3-07.2. *Joint Tactics, Techniques, and Procedures for Antiterrroism.* 17 March 1998.

Joint Task Force – Civil Support (JTF-CS)[U.S. Northern Command] website. Available at http://www.jtfcs.northcom.mil; Internet; Accessed 14 April 2004.

"Joint Task Force-Computer Network Operations." Offutt Air Force Base: U.S. Strategic Command Fact Sheet, 2003. Available from http://www.stratcomaf.mil/factsheetshtml/jtf-cno.htm; Internet; Accessed 25 June 2004.

"Jordan 'was chemical bomb target'." BBC News UK Edition, 17 April 2004. Available at http://news.bbc.co.uk/1/hi/world/middle_east/3635381.stm; Internet; Accessed 28 April 2004.

Kaihla, Paul. "Forging Terror." *Business 2.0* December 2002: 1-3. Available from http://www.business2.com/articles/mag/0,1640,45486%7C5,00.html; Internet; Accessed 22 November 2002.

Kaplan, Robert. *The Coming Anarchy: Shattering the Dreams of the Post Cold War.* New York: Random House, 2000.

Kelley, Jack. "Terror Groups Hide Behind Web Encryption." *USA Today*, 5 February 2001. Available from http://www.usatoday.com/tech/news/2001-02-05-binladen.htm; Internet; Accessed 6 April 2004.

Kurz, Anat. "War Against Terror: United We Stand?" *Jaffee Center for Strategic Studies – Strategic Assessment* 4, no. 4 (February 2002): 1-6. Available from http://www. tau.ac.il/jcss/sa/v4n4p3Kur.html; Internet; Accessed 11 September 2002.

Kushner, Harvey W. *Terrorism in America: A Structured Approach to Understanding the Terrorist Threat.* Springfield, IL. : Charles C. Thomas, Publisher, Ltd., 1998.

Laqueur, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction.* Oxford: Oxford University Press, 1999.

Lasseter, Tom. "Suicide Attackers Strike Karbala," *Knight Ridder,* 27 December 2003. Available from http://www.realcities.com/mld/krwashington/news/special_packages/iraq/7581568.htm; Internet; Accessed 20 January 2004.

Lemos, Robert. "What are the Real Risks of Cyberterrorism?" *ZDNet,* 26 August 2002. Available from http://zdnet.com.com/2102-1105_2-955293.html; Internet; Accessed 6 April 2004.

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare.* Translated by Department of State, American Embassy Beijing Staff Translators. Washington, D.C., 1999.

Long, David E. *The Anatomy of Terrorism.* New York: THE FREE PRESS, A Division of Macmillan, Inc., 1990.

Lowe, Alan C. "Todo o Nada: Montonerosa Versus the Army: Urban Terrorism in Argentina." In *Block by Block: The Challenges of Urban Operations,* ed. William G. Robertson and Lawrence A. Yates. Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2003.

"Man Portable Air Defense System (MANPADS)." *Global Security.org* (n.d.): 1. Available from http://www.globalsecurity.org/military/intro/manpads.htm; Internet; Accessed 19 March 2004.

Manchester, William. *The Arms of Krupp.* Boston: Little, Brown, 1968.

McGuire, Frank G., ed. *Security Intelligence Sourcebook, Including Who's Who in Terrorism.* Silver Spring, MD. : Interests, Ltd., 1990.

MCIA-1100-001-93. *Infantry Weapons Identification Guide.* N.d.

"Medical Uses." *Introduction to Radiological Terrorism,* 3. Available from http://www.nti.org/h_learnmore/radtutorial/chapter01_05.html; Internet; Accessed 19 May 2004.

Michel, Lou and Dan Herbeck. *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing.* New York: Harper Collins Publishers Inc., 2001.

Moilanen, Jon H. "Engagement and Disarmament: A U.S. National Security Strategy for Biological Weapons of Mass Destruction." *Essays on Strategy XIII*. Washington, D.C.; National Defense University, 1996, 141-182.

Molnar, Andrew R. *See* DA Pamphlet 550-104.

Murphy, Shelley. "White Supremacist Accused of Targeting D.C. Museum." *Globe*, 20 September 2001. Available from http://www.rickross.com/reference/supremacists/supremacists57.html; Internet; Accessed 16 February 2004.

Myre, Greg. "Palestinian Bomber, 14, Thwarted before Attack." *International Herald Tribune* March 2004: 1. Available from http://www.iht.com/articles/511745.html; Internet; Accessed 26 March 2004.

National Commission on Terrorist Attacks Upon the United States. Statement of Brian Jenkins to the Commission, March 31, 2003. Available from http://www.9-11commission.gov/hearings/hearing1/witness_jenkins.htm; Internet; Accessed 23 September 2004.

National Response Plan [DHS], Final Draft, 30 June 2004. Available at https://www.niscc.org/download/NRP%20Final%20Draft%2030%20JUN%2004.pdf; Internet; Accessed 4 October 2004.

National Security Institute. *Homeland Security Warns about Vehicle Bombs.* (Medway, MA, n.d.), 1-4. Available from http://nsi.org/Library/Terrorism/Vehicle_Bombs.doc; Internet; Accessed 14 January 2004.

"NE-NE Remote Login Initial Solution Evaluation Criteria." *SONET Interoperability Forum* Document Number SIF-RL-9605-043-R4, (12 June 1996): 4. Available from http://www.atis.org/pub/sif/approved/sif96008.pdf; Internet; Accessed 9 April 2004.

Newman, Bob. "Terrorists Feared to Be Planning Sub-Surface Naval Attacks." *CNS News.com,* 3 December 2002. Available from http://www.cnsnews.com/ForeignBureaus/archive/200212/FOR20021203a.html; Internet; Accessed 19 March 2004.

Newman, David, ed. *Boundaries, Territory and Postmodernity.* Portland: Frank Cass Books, 1999.

Newsday.com, 23 July 1996. Available from http://www.newsday.com/news/nytwa96-jet3bomb,0,2501618.story; Internet; Accessed 12 December 2002.

New York Times, 18 December 1981. "Red Brigades Kidnap an American General in Verona.".

New York Times, 13 January 2003. Available from http://www.nytimes.com/2003/01/13/ politics/13INTE.html; Internet; Accessed 13 January 2003.

"Oklahoma Bombing Chronology." *Washington Post.* Available from http://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/chron.htm; Internet; Accessed 5 March 2004.

Oman, Paul, and Edmund Schweitzer, and Jeff Roberts, "Protecting the Grid from Cyber Attack Part I: Recognizing Our Vulnerabilities." *Utility Automation and Engineering T&D*, November 2001. Available from http://uaelp.pennnet.com; Internet; Accessed 24 June 2004.

Ong, Graham Gerard. "Next Stop, Maritime Terrorism." *Viewpoints* (12 September 2003): 1-2. Available from http://www.iseas.edu.sg/viewpoint/ggosep03.pdf; Internet; Accessed 2 April 2004.

"Operation Winter Harvest: The Rescue of Brigadier James Dozier." *Special Operations. Com*. Available from http://www.specialoperations.com/Counterterrorism/Dozier.html; Internet; Accessed 26 February 2004.

Pawle, Gerald. *Secret Weapons of World War II*. New York: Ballantine Books, 1967.

Paz, Reuven. *Hamas Publishes Annual Report on Terrorist Activity for 1998.* Herzliya, Israel: International Policy Institute for Counterterrorism, May 3, 1999. Available from http://www.ict.org.il/spotlight/det.cfm?id=259; Internet; Accessed 6 December 2002.

Perl, Raphael and Ronald O'Rourke. *"Terrorist Attack on USS Cole: Background and Issues for Congress."* Congressional Research Service, The Library of Congress. Order Code RS20721, 1. 30 January 2001. Available from http://news.findlaw.com/cnn/docs/crs/coleterrattck13001.pdf; Internet; Accessed 5 April 2004.

Phillips, Thomas D. "The Dozier Kidnapping: Confronting the Red Brigades." *Air & Space Power Chronicles* (February 2002): 1. Available from http://www.airpower.maxwell/af.mil/airchronicles/cc/phillips.html; Internet; Accessed 31 March 2004.

Popenker, Max R. *Modern Firearms and Ammunition.* [Encyclopedia online]. N.p., n.d. Available from http://world.guns.ru/main-e.htm#md; Internet; Accessed 31 October 2002.

Poulsen, Kevin. "Rumsfeld Orders .mil Web Lockdown." *The Register*, 17 January 2003. Available from http://www.theregister.co.uk/2003/01/17/rumsfeld_orders_mil_web_lockdown; Internet; Accessed 8 April 2004.

Powell, William. *The Anarchist Cookbook.* Secaucus, NJ: Lyle Stuart, Inc., 1971.

Prados, Alfred B. Congressional Research Service (CRS) Issue Brief for Congress. *Saudi Arabia: Current Issues and U.S. Relations*, 15 September 2003. Order Code IB93113.

Quinn, Andrew. "Teen Hackers Plead Guilty to Stunning Pentagon Attacks." *Reuters*, 31 July 1998, 1. Available from http://www.geocities.com/Area51/Shadowlands/6583/project395.html; Internet; Accessed 14 April 2004.

Ra'anan, Uri, ed., et al. *Hydra of Carnage: International Linkages of Terrorism.* Lexington: Lexington Books, 1986.

Rapoport, David C., ed. *Inside Terrorist Organizations*. New York: Columbia University Press, 1988.

Raufer, Xavier. "New World Disorder, New Terrorisms: New Threats for the Western World." In *The Future of Terrorism*, edited by Max. Taylor and John Horgan. Portland: Frank Cass Publishers, 2000.

Reich, Walter, ed. *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*. Rev. ed. Washington: Woodrow Wilson Center Press, 1998.

"Revolutionary Organization 17 November (17N)." CDI Terrorism Project, 5 August 2002. Available from http://www.cdi.org/terrorism/17N-pr.cfm; Internet; Accessed 24 September 2004.

Richardson, Michael. "A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction." *Viewpoints* (25 February 2004): 8. Available from http://www.iseas.edu.sg/viewpoint/mricsumfeb04.pdf; Internet; Accessed 5 April 2004.

Robinson, Colin. *Military and Cyber-Defense: Reactions to the Threa.t* Washington: Center for Defense Information Terrorism Project, 2002. Available from http://www.cdi.org/terrorism/cyberdefense-pr.cfm; Internet; Accessed 24 June 2004.

Rosenbraugh, Craig. "Craig Rosenbraugh on the Anti-War Struggle." *Houston Independent Media Center*, 17 March 2003. Available from http://houston.indymedia.org/news/2003/03/9125.php ; Internet; Accessed 16 February 2004.

"Ruby Ridge Federal Siege, Bibliography." [Bibliography on-line]. Available from http://users.skynet.be/terrroism/html/usa_ruby_ridge.htm; Internet; Accessed 16 March 2004.

Rumsfeld, Donald H. *See* U.S. Department of Defense.

St. Petersburg Times, 9 December 1999. Dougherty, Larry. "Indictment details plot to blow up power lines." Available from http://www.sptimes.com/News/120999/TampaBay/Indictment_details_pl.shtml; Internet; Accessed 16 February 2004.

"SAMs and the Targeting of Israeli Airliners." *Jane's Terrorism Intelligence Center* (28 November 2002): 1. Available from http://www.janes.com/security/international_security/news/jtic/jtic021128_1_n.shtml; Internet; Accessed 30 December 2002.

Schama, Simon. *Citizens: A Chronicle of The French Revolution.* New York: Alfred A. Knopf, Inc., 1989.

Schuurman, Jan. *Tourists or Terrorists?* Press review on-line. Radio Netherlands, 25 April 2002. Available from http://www.rnw.nl/hotspots/html/irel020425.html; Internet; Accessed 13 February 2004.

Schweitzer, Glenn E., and Carole C. Dorsch. *Superterrorism; Assassins, Mobsters, & Weapons of Mass Destruction.* New York: Plenum Trade Press, 1998.

Schweitzer, Yoram. "Suicide Terrorism: Development and Main Characteristics." In *Countering Suicide Terrorism.* Herzilya, Israel: The International Policy Institute for Counter Terrorism, The Interdisciplinary Center, 2002.

Serrano, Richard A. "Terry Nichols Sentenced to Life With No Hope of Parole." *Los Angeles Times*, 5 June 1998. Available from http://www.-tech.mit.edu/V118/N27/nichols.27w.htm; Internet; Accessed 16 February 2004.

Silverstein, Ken. "David Hahn, Boy Atomic Scientist." *ASEPCO*, [Originally printed in *Harpers's Magazine*, November 1998]. Available at http://www.asepco.com/David_Hahn_Boy_Scientist.htm.; Internet; Accessed 31 August 2004.

Simons, Lewis M. "Weapons of Mass Destruction: An Ominous New Chapter Opens on the Twentieth Century's Ugliest Legacy." *National Geographic* 202, no. 5 (November 2002): 2-35.

Smith, Brent L. *Terrorism in America: Pipe Bombs and Pipe Dreams.* Albany: State University of New York Press, 1994.

"Software - Programming Jobs are Heading Overseas by the Thousands. Is there a Way for the U.S. to Stay on Top?" *BusinessWeek online*, 1 March 2004. Available from http://businessweek.com/magazine/content/04_09/b3872001_mz001.htm; Internet; Accessed 9 April 2004.

"Sprint Inks Outsouring Pacts with EDS, IBM." *Dallas Business Journal,* (16 September 2003). Available from http://www.bizjournals.com/dallas/stories/2003/09/15/daily21.html; Internet; Accessed 9 April 2004.

Sprinzak, Ehud. "Rational Fanatics." *Foreign Policy,* no. 120 (September/October 2000): 66-73.

Straits Times Interactive, 16 October 2003. Rekhi, Shefali. "Next terror target." Available from http://www.google.com/search?hl=en&lr=&ie=UTF-8&q=terrro+AND+attack+AND=underwater&btnG=Google+Search; Internet; Accessed 21 January 2004.

Suicide Terror: It's Use and Rationalization. Jerusalem: Israeli Ministry of Foreign Affairs Website, 23 July 2002. Available from http://www.mfa.gov.il/mfa/ go.asp? MFAH0m6k0; Internet; Accessed 11 November 2002.

"Suicide Terrorism." *The Economist* (January 2004): 3. Available from http://quicksitebuilder.cnet.com/supfacts/id396.html; Internet; Accessed 17 March 2004.

"Suicide Terrorism in Comparative Perspective." In *Countering Suicide Terrorism.* Herzilya, Israel: The International Policy Institute for Counter Terrorism, The Interdisciplinary Center, 2002.

"Suicide Terrorism: a Global Threat." *Jane's Intelligence Review* (October 2000): 1, 4-5. Available from http://www.janes.com/security/international_security/news/usscole/jir001020_1_n.shtml; Internet; Accessed 20 January 2004.

Sullivan, John P., et al. *Jane's Unconventional Weapons Response Handbook.* Alexandria, VA: Jane's Information Group, 2002.

Sunzi. *The Art of War/Sun Tzu*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1971.

Tal, Nachman. "Suicide Attacks: Israel and Islamic Terrorism." *Jaffee Center for Strategic Studies – Strategic Assessment* 5, no. 1 (June 2002): 1-9.

Taylor, Max, and John Horgan, ed. *The Future of Terrorism*. Portland: Frank Cass Publishers, 2000.

Teitelbaum, Joshua and David Long. "Islamic Politics in Saudi Arabia." *The Washington Institute for Near East Policy, Policywatch:* Special Policy Forum Report Number 259, 9 July 1997, 1 to 3. Available at http://www.washingtoninstitute.org/watch/Policywatch/policywatch1997/259.htm; Internet; Accessed 19 February 2004.

"Terrorist Attacks on Americans 1979-1988." 2. Available from http://www.pbs.org/wgbh/pages/frontline/shows/target/etc/cron.html; Internet; Accessed 1 July 2004

"Terrorists Demand Extortion Cash in Euros." *TCM Breaking News* (September 2001): 1. Available from http://archives.tcm.ie/breakingnews/2001/09/04/story22584.asp; Internet; Accessed 31 March 2004.

"Terrorists and Radiological Terrorism." *Introduction to Radiological Terrorism,* 2 and 3. Available from http://www.nti.org/h_learnmore/radtutorial/chapter04_02.html; Internet; Accessed 19 May 2004.

Thachuck, Kimberly L. "Terrorism's Financial Lifeline: Can it Be Severed." *Strategic Forum* no. 191 (May 2002): 1-15. Available from http://www.ndu.edu/inss/strforum/sf191.htm; Internet; Accessed 29 August 2002.

"The Asymmetric Threat From Maritime Terrorism." Available from http://jfs.janes.com/public/jfs/additional_info.shtml; Internet; Accessed 2 February 2004.

"The New Threat of Organized Crime and Terrorism." *Jane's Terrorism & Security Monitor* (6 June 2000): 1-5. Available from http://www.janes.com/security/international_security/ news/jtsm/jtsm000619_1_n.shtml; Internet; Accessed 27 June 2000.

The *Posse Comitatus Act*, 18 U.S.C. 1385

The *Robert. T. Stafford Disaster Relief and Emergency Assistance Act*, 42 U.S.C. 5121-5206

The White House. National Security Presidential Directive 17 (NSPD-17), *National Strategy to Combat Weapons of Mass Destruction*, 2, December 2002. Available at http://www.fas.org/irp/offdocs/nspd/nspd-17.html; Internet; Accessed 8 December 2003.

The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* Washington, D.C., February 2003. Preface by The President of the United States of America. Available from http://www.whitehouse.gov/pcipb/physical_strategy.pdf; Internet; Accessed 8 December 2003.

The White House. *The National Security Strategy of the United Sates of America*, 1, 17 September 2002. Available at http://www.whitehouse.gov/nsc/nss.html; Internet; Accessed 30 April 2004.

The White House. *The National Strategy to Secure Cyberspace.* Washington, D.C., February 2003. Preface by The President of the United States of America. Available from http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf; Internet; Accessed 8 December 2003.

TM 31-201-1. *Unconventional Warfare Devices and Techniques: Incendiaries.* May 1966.

TM 31-210. *Improvised Munitions Handbook.* 1969.

"Too Painful." *ABC News.* News on-line, 11 November 2004. Available from
    http://abcnews.go.com/sections/Primetime/US/Jessica_Lynch_031106-1.html; Internet; Accessed 12
    February 2004.

"Transcript of President George Bush's Address 10/07/01. 'Attack on America'." Available
    http://multimedia.belointeractive.com/attack/bush/1007bushtranscript.html; Internet; Accessed 13 July 2004.

Truby, J. David. *How Terrorists Kill: The Complete Terrorist Arsenal.* Boulder: Paladin Press, 1978.

USAEUR Pamphlet 30-60-1. *Identification Guide: Part One, Weapons and Equipment East European
    Communist Armies; Volume I: General, Ammunition and Infantry Weapons.* 30 September 1972.

U.S. Air Force. *Independent Review of the Khobar Towers Bombing, Part A* (31 October 1996) by Lieutenant
    General James F. Record. Available from http://www.fas.org/irp/threat/khobar_af/recordf.htm; Internet;
    Accessed 9 February 2004.

U.S. Air Force. *Independent Review of the Khobar Towers Bombing, Part A; Appendix 1, Comments Regarding
    the Downing Report* (31 October 1996) by Lieutenant General James F. Record. Available from
    http://www.fas.org/irp/threat/khobar_af/recordap.htm; Internet; Accessed 9 February 2004.

U.S. Congress. House. Armed Services Special Oversight Panel on Terrorism, *Cyberterrorism*, Testimony by
    Dorothy E. Denning, Georgetown University. Washington, D.C., 23 May 2000. Available from
    http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Internet; Accessed 9 April 2004.

U.S. Congress. House. Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities.
    Cyber-Terrorism. Statement by Major General James D. Bryan, U.S. Army Commander, Joint task Force-
    Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems
    Agency. Washington, D.C., 24 July 2003. Available from http://www.defenselink.mil/search97/s97is.vts?
    Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; Accessed 6 April 2004.

U.S. Congress. House. Resources Subcommittee on Forests and Forest Health. *The Threat of Eco-Terrorism.*
    Statement by the FBI's Domestic Terrorism Section Chief, James Jarboe. Washington, D.C., 12 February
    2002. Available from http://www.fbi.gov/_congress/congress02/jarboe021202.htm; Internet; Accessed 17
    January 2003.

U.S. Congress. Senate. Armed Services Committee. *SASC Cole Commission Testimony: Hearing before the
    Armed Services Committee.* 107th Cong. 3 May 2001. Comments by Chairman of the Joint Chiefs of Staff.

U.S. Congress. Senate. Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, Cyber
    Terrorism. Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, Washington,
    D.C., 24 February 2004, 3. Available from http://www.fbi.gov/congress/congress04/lourdeau022404.htm;
    Internet; Accessed 15 April 2004.

U.S. Department of Agriculture. "Final BSE Update – Monday, February 9, 2004." Newsroom Release
    Statement No. 0074.04. Available from http://www.usda.gov/Newsroom/0074.04.html; Internet; Accessed
    12 July 2004.

U.S. Department of Commerce. National Institute of Standards and Technology, *Risk Management Guide for
    Information Technology Systems,* NIST Special Publication 800-30, by Gary Stoneburner, Alice Goguen,
    and Alexis Feringa. Washington, D.C., 2001: 22. Available from
    http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf; Internet; Accessed 12 April 2004.

U.S. Department of Defense. *11th Psychological Operations Task Force After Action Report for SFOR X*, by
    Clint A. Venekamp. Upper Marboro, MD, July 2002.

U.S. Department of Defense. "A Global Terror Group Primer," by Jim Garamone. *Defense Link* (14 February 2002): 1-7. Available from http://www.defenselink.mil/news/_Feb2002/n02142002_200202141.html; Internet; Accessed 29 August 2002.

U.S. Department of Defense. Defense Security Service, Technology Collection Trends in the U.S. Defense Industry 2002. Alexandria, VA, n.d. Available from http://www.wright.edu/rsp/Security/TechTrends.pdf; Internet; Accessed 19 April 2004.

U.S. Department of Defense. *DoD USS Cole Commission Report* (9 January 2001) by U.S. Army Gen. (Ret) William Crouch and U.S. Navy Adm. (Ret) Harold Gehman. Open-File Report, U.S. Department of Defense. 1 (Washington, D.C., 9 January 2001). Available at http://www.fas.org/irp/threat/cole.html; Internet; Accessed 16 February 2004.

U.S. Department of Defense. Naval Explosive Ordnance Disposal Technology Division. *ORDATA II - Enhanced Deminers' Guide to UXO Identification, Recovery, and Disposal,* Version 1.0, [CD-ROM]. Indian Head, MD: Naval Explosive Ordnance Disposal Technology Division, 1999.

U.S. Department of Defense. News Release Archive. "DoD News: Navy Announces Results of Its Investigation on USS Cole." Available from http://www.defenselink.mil/releases/2001/b011192001_bt031-01.html; Internet; Accessed 11 February 2004.

U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) Letter by General (USA Retired) Wayne A. Downing. Available from http://www.fas.org/irp/threat/downing/downltr.html; Internet; Accessed 10 February 2004.

U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Pre by Wayne A. Downing. Available from http://www.fas.org/irp/threat/downing/prefuncl.html; Internet; Accessed 10 February 2004.

U.S. Department of Defense. *Report of the Assessment of the Khobar Towers Bombing* (30 August 1996) by General (USA Retired) Rpt by Wayne A. Downing. Available from http://www.fas.org/irp/threat/downing/unclf913.html; Internet; Accessed 9 February 2004.

U.S. Department of Defense. *Report to Congress on The Role of the Department of Defense in Supporting Homeland Security.* Washington, D.C., September 2003.

U.S. Department of Defense. *Report on Personal Accountability for Force Protection at Khobar Towers*, by William S. Cohen. Washington, D.C., July 31, 1997.

U.S. Department of Defense. Report to the President. *The Protection of U.S. Forces Deployed Abroad* (15 September 1996) by Secretary of Defense William J. Perry. Available from http://www.fas.org/irp/threat/downing/report_f.html; Internet; Accessed 18 February 2004.

U.S. Department of Defense. *Special Briefing on the Unified Command Plan*, by Donald H. Rumsfeld. Department of Defense News Briefing Transcript presented at the Pentagon, Wednesday, 17 April 2002 – 11:30a.m. Available from http://www.defenselink.mil/ news/Apr2002/t04172002_t0417sd.html; Internet; Accessed 18 November 2002.

U.S. Department of Defense. Threat Support Directorate TRADOC DCSINT. *Homeland Defense Handbook*. Fort Leavenworth, KS, 31 October 2001.

U.S. Department of Defense. Threat Support Directorate TRADOC DCSINT. *OPFOR Worldwide Equipment Guide*. Fort Leavenworth, KS, 24 September 2001.

U.S. Department of Defense. U.S. Army John F. Kennedy Center for Special Warfare. *U.S. Army Special Forces Foreign Weapons Handbook*. Fort Bragg, N.C., 1 January 1967.

U.S. Department of Defense. U.S. Army Intelligence Agency. Foreign Science and Technology Center. (S/NF/WN/NC) *Terrorist Weapons Handbook – Worldwide* (U), by Steven A. Chester. Washington, D.C., 15 December 1989. [Unclassified extract].

U.S. Department of Defense. U.S. Marine Corps. Marine Corps University. Corporals Noncommissioned Officers Program. *Force Protection.* Quantico, VA, January 1999.

U.S. Department of Defense. Washington Headquarters Services. Directorate for Information Operations and Reports. *Global War on Terrorism – Casualty Summary Operation Enduring Freedom.* Washington, D.C., As of 4 March 2004. Available from http://web1.whs.osd.mil/mmid/casualty/WOTSUM.pdf; Internet; Accessed 15 March 2004.

U.S. Department of Defense. Washington Headquarters Services. Directorate for Information Operations and Reports. *Table 13, Worldwide U.S. Active Duty Military Deaths, Selected Military Operations.* Washington, D.C., n.d. Available from http://web1.whs.osd.mil/mmid/casualty/table13.htm; Internet; Accessed 15 March 2004.

U.S. Department of Defense. Washington Headquarters Services. Directorate for Information Operations and Reports. *U.S. Active Duty Military Deaths – 1980 through 2002.* Washington, D.C., As of 10 April 2003. Available from http://web1.whs.osd.mil/mmid/casualty/Death_Rates.pdf; Internet; Accessed 16 January 2004.

U.S. Department of Defense. Washington Headquarters Services. Directorate for Information Operations and Reports. *War on Terrorism – Operation Iraqi Freedom, By Casualty Category within Type.* Washington, D.C., As of 26 February 2004. Available from http://web1.whs.osd.mil/mmid/casualty/OIF-Total.pdf; Internet; Accessed 15 March 2004.

U.S. Department of Justice. "Al Qaeda Associates Charged in Attack on USS Cole, Attempted Attack on Another U.S. Naval Vessel." Public Relations Release #298: 05-15-03, 3. 15 May 2003. Available on Http://www.usdoj.gov/opa/pr/2003/May/03_298.htm; Internet; Accessed 16 February 2004.

U.S. Department of Justice. Federal Bureau of Investigation. Counterterrorism Threat Assessment and Warning Unit. Counterterrorism Division. *Terrorism in the United States 1999.* Report 0308. Washington, D.C., n.d.

U.S. Department of Justice. Office of Justice Programs. Office for Victims of Crime. *Responding to Terrorism Victims* (October 2000), by Kathryn M. Turman, Director. Available at http://www.ojp.usdoj.gov/ovc//publications/infores/respterrorism/welcome.html; Internet; Accessed 11 March 2004.

U.S. Department of Justice. U.S. Attorney, Northern District of California. Press Release, *Louisiana Man Arrested for Releasing 911 Worm to WebTV Users*, (San Francisco, CA, 19 February 2004), 1. Available from http://www.usdoj.gov/criminal/cybercrime/jeansonneArrest.htm; Internet; Accessed 12 April 2004.

U.S. Department of Justice. U.S. Attorney, Southern District of California. Press Release, *President of San Diego Computer Security Company Indicted in Conspiracy to Gain Unauthorized Access into Government Computer.* San Diego, CA, 29 September 2003. Available from http://www.usdoj.gov/criminal/cybercrime/okeefeArrest.htm; Internet; Accessed 12 April 2004.

U.S. Department of Justice. U.S. District Court for the Eastern District of Virginia. Alexandria Division, Indictment, *United States of America v. Gary McKinnon.* Alexandria, VA, November 2002. Available from http://news.findlaw.com/hdocs/docs/cyberlaw/usmck1102vaind.pdf; Internet; Accessed 16 April 2004.

U.S. Department of State. Bureau of Diplomatic Security. *State Department Diplomatic Security Surveillance Detection Program Course of Instruction* [CD-ROM]. Washington, D.C., October 1999.

U.S. Department of State. "Clinton Letter to Congress on U.S.S. Cole Attack." *International Information Programs, Washington File.* Available from http://usinfo.state.gov/topical/pol/terrro/00101603.htm; Internet; Accessed 1 April 2004.

U.S. Department of State. International Information Programs Bulletin. *Justice Department on Khobar Towers Explosion Indictments,* 21 June 2001. Available from http://usinfo.state.gov/topical/pol/terror/01062102.htm; Internet; Accessed 10 February 2004.

U.S. Department of State. Office of the Coordinator for Counterterrroism. *Patterns of Global Terrorism 2001.* Washington, D.C., May 2002.

U.S. Department of State. Office of the Coordinator for Counterterrorism. *Patterns of Global Terrorism 2002.* Washington, D.C., 2003.

U.S. Department of State. Office of the Coordinator for Counterterrorism. *Patterns of Global Terrorism 2004.* Washington, D.C., 2004, revised 22 June 2004.

U.S. Department of State. Office of Counterterrorism. *Foreign Terrorist Organizations.* Washington, D.C., 9 August 2002. Available from http://www.state.gov/s/ct/rls/fs/_2002/12389.htm; Internet; Accessed 29 August 2002.

U.S. Department of State. Office of the Historian. Bureau of Public Affairs. *Significant Terrorist Incidents, 1961-2001: A Chronology.* Washington, D.C., 31 October 2001. Available from http://www.fas.org/irp/threat/terror_chron.html; Internet; Accessed 30 January 2003.

U.S. Department of State. U.S. Embassy, Jakarta, Indonesia. *Threats Involving Vehicle Borne Improvised Explosive Devices.* Jakarta, Indonesia, 2003, 2. Available from http://www.usembassyjakarta.org/vbied_vehicles.html; Internet; Accessed 14 January 2004.

U.S. Department of the Treasury. Office of the Comptroller of the Currency. *Infrastructure Threats from Cyber-Terrorists*, OCC Bulletin 99-9. Washington, D.C., 5 March 1999, 2. Available from http://www.occ.treas.gov/ftp/bulletin/99-9.txt; Internet; Accessed 6 April 2004.

U.S. Director of Central Intelligence. DCI Counterterrorist Center. *International Terrorism in 1997: A Statistical View.* Washington, D.C., 1998. Available from http://www.fas.org/irp/threat/terror97cia; Internet; Accessed 3 February 2003

U.S. Director of Central Intelligence. DCI Weapons Intelligence. Nonproliferation, and Arms Control Center. *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2001.* Washington, D.C., January 2002.

U.S. Director of Central Intelligence. Interagency Intelligence Committee on Terrorism. Chemical, Biological and Radiological (CBRN) Subcommittee. *Chemical/Biological/Radiological Incident Handbook.* Washington, D.C., October 1998. Available from http://images.google.com/imgres?imgurl=www.usis.usemb.se/ Environment/images/p1.gif&imgrefurl=http://www.usis.usemb.se/Environment/&h=158&w=168&prev=/images%3Fq%3Dus%2Bgovernment%26svnum%3D10%26hl%3Den%26lr%3D%26ie%3DUTF-8%26oe%3DUTF-8; Internet; Accessed 13 February 2003.

U.S. Director of Central Intelligence. Interagency Intelligence Committee on Terrorism. Community Counterterrorism Board. (FOUO) *Improvised Explosive Devices (IEDs) and Other Criminal and Terrorist Devices: A Basic Reference Manual.* Washington, D.C., September 2000.

U.S. District Court, District of Colorado. Criminal Action No. 95-CR-110. United States of America, Plaintiff, vs. Timothy James McVeigh and Terry Lynn Nichols, Defendants. "8/95 Grand Jury Indictment of McVeigh and Nichols." Indictment Count One (Conspiracy to Use a Weapon of Mass Destruction), 1995, 1. Available from http://www.lectlaw.com/files/cas44.htm; Internet; Accessed 2 February 2004.

U.S. District Court, District of Colorado. Criminal Action No. 96-CR-68. United States of America, Plaintiff, vs. Timothy James McVeigh, Defendant. The McVeigh Trial's April 24, 1997 Opening Statement by the [U.S.] Government. Available from http://www.lectlaw.com/bomb.html; Internet; Accessed 5 March 2004.

U..S. District Court, Eastern District of Virginia, Alexandria Division. Grand Jury *Indictment* of 46 counts against named and unspecified terrorists charged in the Khobar Towers bombing attack of 25 June 1996. Available from http://www.fbi.gov/pressrel/pressrel01/khobar.pdf; Internet; Accessed 10 February 2004.

U.S. District Court, Southern District of New York. Indictment S12 98 Cr. 1023 (KTD). United States of America, Plaintiff, vs. Jamal Ahmed Mohammed Ali Al-Badawi and Fahd Al-Quso, Defendants. Available from http://news.findlaw.com/hdocs/docs/cole/usalbadawi051503ind.pdf; Internet; Accessed 5 April 2004.

U.S. District Court, Western District of Oklahoma. Case No. M-95-105-H. United States of America. Plaintiff, vs. Terry Lynn Nichols, Defendant. "Terry Nichols Criminal Complaint." Affidavit. 9 May 1995, 2. Available from http://www.lectlaw.com/files/cur18.htm; Internet; Accessed 16 February 2004.

U.S. District Court, Western District of Oklahoma. Case No. M-95-105-H. United States of America. Plaintiff, vs. Michael J. Fortier, Defendant. "Michael Fortier's Plea Agreement." Affidavit. 10 August 1995, 2. Available from http://www.lectlaw.com/files/cas37.htm; Internet.; Accessed 16 February 2004.

U.S. General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84. Washington, D.C., 22 May 1996. Available from http://www.fas.org/irp/gao/aim96084.htm; Internet; Accessed 12 April 2004.

U.S. House National Security Committee. *Report on the Bombing of Khobar Towers* 14 August 1996. Statement of Chairman Floyd D. Spence and Staff Report. Available from http://www.fas.org/irp/threat/saudi.pdf; Internet; Accessed10 February 2004.

USNORTHCOM [U.S. Northern Command] website. Available at http://www.northcom.mil; Internet; Accessed 28 April 2004.

"U.S. Officials Charge Briton for Hacking Pentagon." *Asian School of Cyber Laws,* November 2002. Available from http://www.asianlaws.org/cyberlaw/archives/11_02_penta.htm; Internet; Accessed 16 April 2004.

U.S. Title 28. Code of Federal Regulations. Section 0.85. *Judicial Administration*. Washington, D.C., July 2001.

Van Creveld, Martin L. *The Transformation of War*. New York: The Free Press, 1991.

Venekamp, Clint A. *See* U.S. Department of Defense.

Venzke, Ben N. *Al-Qaeda Targeting Guidance – v1.0, Thursday 1 April 2004*. Alexandria: IntelCenter/Tempest Publishing, 2004.

Venzke, Ben N., and Aimee Ibrahim. *Al-Qaeda Tactic/Target Brief*. Alexandria: Intel Center/Tempest Publishing, 2002.

_____. *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets.* Alexandria: Tempest Publishing, LLC, 2003, 36, quoting Abu 'Ubeid al-Qurashi, "The Nightmares of America, 13 February 2002.

von Clausewitz, Karl. *War, Politics and Power.* Chicago: Regnery Gateway, 1962.

Vinocur, John. "Bomb Attempt on Gen. Haig's Life Not Tied to Major Terrorist Groups." *New York Times*, 27 June 1979.

_____. "U.S. General Safe in Raid in Germany." *New York Times*. 16 September 1981.

"Waco – Branch Davidian Files." Available from http://www.paperlessarchives.com/waco.html; Internet; Accessed 16 March 2004.

Wagamon, Ed. "Tactical Combat in Chechnya: Mines & Booby Traps: The Number One Killer" (Part 1 of 2). *How They Fight: Armies of the World,* NGIC-1122-0062-01, vol 4-01 (August 2001): 33-37.

Walsh, Elsa. "Louis Freech's Last Case." *The New Yorker*, 14 May 2001. Available from http://www.newyorker.com/printable/?archive/010924fr_archive06; Internet; Accessed 12 February 2004.

The War on Terrorism: The U.S. and the S.P.L.A. London: The European-Sudanese Public Affairs Council Press Release, 12 October 2001. Available from http://allafrica.com/stories/200110120528.html; Internet; Accessed 12 November 2002.

Washington Times.com. 1 December 2003. Available from http://www.washtimes.com/upi-breaking/20031201-025645-3524r.htm; Internet; Accessed 2 April 2004.

Weapons of Mass Destruction. New York: United Nations Office on Drugs and Crime, December 2002. Available from http://www.undcp.org/odccp/terrorism_weapons___mass_destruction_page006.html; Internet; Accessed 19 December 2002.

"Weapons of Terror." *ADL* (8 April 2002): 1. Available from http://www.adl.org/_israel/weapons_list.asp; Internet; Accessed 8 January 2003.

West, Woody. "The Last Word." *Insight: On the News,* 16 November 2001. Available from http://www.insightmag.com/news/2001/12/10/Features/The-Last-Word-148069.shtml; Internet; Accessed 12 February 2004.

"What is Radiological Terrorism?" *Introduction to Radiological Terrorism,* 1 and 2. Available from http://www.nti.org/h_learnmore/radtutorial/chapter01_03.html; Internet; Accessed 19 May 2004.

White, Jerry. "Ridding the World of Land Mines." *Union-Tribune* (January 24, 2002): 4-5. Available from http://www.wand.org/9-11/discuss6.html; Internet; Accessed 13 December 2002.

Williscroft, Robert G. "The Economics of Demining Defines Success and Failure." *Defense Watch* February 13, 2002: 1-17. Available from http://www.sftt.org/_dw02132002.html; Internet; Accessed 13 December 2002.

Zakis, Jeremy. *Annual Report of International Terrorist Activity, 2001*. Chicago: The Emergency Response and Research Institute, 2002. Available from http://www._emergency.com/2002/erri_ter2001.pdf; Internet; Accessed 7 November 2002

Page Intentionally Blank

"The battle is now joined on many fronts.
We will not waiver, we will not tire,
we will not falter, and we will not fail.
Peace and freedom will prevail…
To all the men and women in our military,
every sailor, every soldier, every airman,
every coast guardsman, every marine,
I say this: Your mission is defined.
The objectives are clear. Your goal is just.
You have my full confidence, and you will have
every tool you need to carry out your duty."

George W. Bush
President
United States of America

A Military Guide to Terrorism in the Twenty-First Century
US Army Training and Doctrine Command
Deputy Chief of Staff for Intelligence
Assistant Deputy Chief of Staff for Intelligence-Threats
Fort Leavenworth, Kansas